

(19)

(11) Publication number: 2003101527 A

Generated Document

PATENT ABSTRACTS OF JAPAN

(21) Application number: 2001286881

(51) Int'l. Cl.: H04L 9/10 G06F 12/14

(22) Application date: 20.09.01

(30) Priority:

(43) Date of application 04.04.03
publication:

(84) Designated
contracting states:

(71) Applicant: MATSUSHITA ELECTRIC IND CO LTD

(72) Inventor: FUJIWARA MUTSUMI
NEMOTO YUSUKE

(74) Representative:

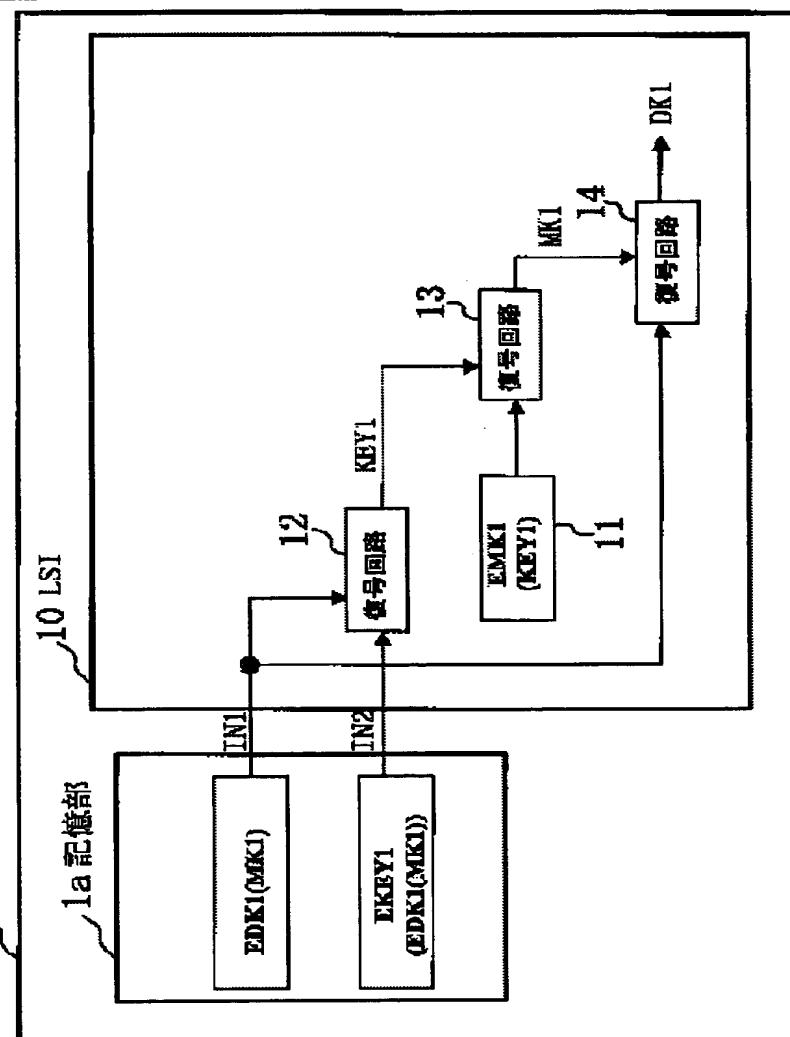
(54) KEY MOUNTING SYSTEM
AND LSI FOR IMPLEMENTING
THE SAME, AS WELL AS KEY
MOUNTING METHOD

(57) Abstract:

PROBLEM TO BE SOLVED: To
improve secrecy and concealment
for a key in a key mounting system.

SOLUTION: A decryption circuit 12
decrypts an encrypted key EKEY1
(EDK1(MK1)) using an encrypted
key EDK1(MK1) as a key, and a
decryption circuit 13 decrypts an
encrypted key EMK1 (KEY1) using
the output of the decryption circuit
12, namely an internal key KEY1, as
a key. A decryption circuit 14
decrypts the encrypted key EDK1
(MK1) using the output of the
decryption circuit 13, namely an
internal key MK1 as a key, and
generates a final key DK1. Namely,
all of the keys mounted on a
storage unit 1a and an LSI 10 are
encrypted. Moreover, the final key
DK1 is generated at the LSI 10.

COPYRIGHT: (C)2003,JPO



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2003-101527
(P2003-101527A)

(43)公開日 平成15年4月4日 (2003.4.4)

(51)Int.Cl.
H 04 L 9/10
G 06 F 12/14

識別記号
3 2 0

F I
G 06 F 12/14
H 04 L 9/00

テマコード(参考)
3 2 0 B 5 B 0 1 7
6 2 1 A 5 J 1 0 4

審査請求 未請求 請求項の数20 OL (全 26 頁)

(21)出願番号 特願2001-286881(P2001-286881)

(22)出願日 平成13年9月20日 (2001.9.20)

(71)出願人 000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者 藤原 瞳
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
(72)発明者 根本 祐輔
大阪府門真市大字門真1006番地 松下電器
産業株式会社内
(74)代理人 100077931
弁理士 前田 弘 (外7名)

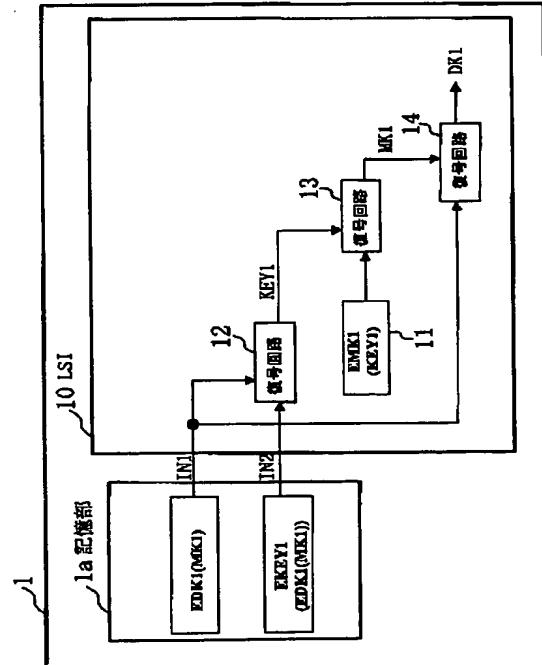
最終頁に続く

(54)【発明の名称】 鍵実装システムおよびこれを実現するためのLSI、並びに鍵実装方法

(57)【要約】

【課題】 鍵実装システムにおいて、鍵の機密性および
秘匿性をより向上させる。

【解決手段】 復号回路12は被暗号化鍵E KEY1
(EDK1 (MK1))を被暗号化鍵EDK1 (MK
1)を鍵として復号化し、復号回路13は被暗号化鍵E
MK1 (KEY1)を、復号回路12の出力すなわち内
部鍵KEY1を鍵として復号化する。復号回路14は被
暗号化鍵EDK1 (MK1)を、復号回路13の出力す
なわち内部鍵MK1を鍵として復号化し、最終鍵DK1
を生成する。すなわち、記憶部1aおよびLSI10に
実装された鍵は全て暗号化されたものであり、しかも、
LSI10で最終鍵DK1が生成される。



【特許請求の範囲】

【請求項1】 記憶部と、LSIとを有する鍵実装システムであって、
前記記憶部は、
最終鍵を、第1の内部鍵を用いて暗号化して得た第1の被暗号化鍵と、
第2の内部鍵を、前記第1の被暗号化鍵を用いて暗号化して得た第2の被暗号化鍵とを記憶しており、
前記LSIは、
前記第1の内部鍵を、前記第2の内部鍵を用いて暗号化して得た第3の被暗号化鍵を記憶しており、前記記憶部から、前記第1および第2の被暗号化鍵を入力するものであり、かつ、
入力された第2の被暗号化鍵を、入力された第1の被暗号化鍵を鍵として用いて復号化する第1の復号回路と、前記第3の被暗号化鍵を、前記第1の復号回路の出力を鍵として用いて復号化する第2の復号回路と、
入力された第1の被暗号化鍵を、前記第2の復号回路の出力を鍵として用いて復号化する第3の復号回路とを備えたものであることを特徴とする鍵実装システム。
【請求項2】 請求項1において、前記LSIは、
第1のテスト用内部鍵を、第2のテスト用内部鍵を用いて暗号化して得た第4の被暗号化鍵をさらに記憶しており、かつ、
前記第3および第4の被暗号化鍵を入力とし、このいずれかを、第1のテスト信号に応じて選択出力する第1のセレクタと、
前記第1のセレクタの選択出力と、前記第2の復号回路の出力をとを入力とし、このいずれかを、第2のテスト信号に応じて選択出力する第2のセレクタとを備え、
前記第2の復号回路は、前記第3の被暗号化鍵の代わりに、前記第1のセレクタの出力を入力とするものであり、
前記第3の復号回路は、前記第2の復号回路の出力の代わりに、前記第2のセレクタの出力を鍵として入力するものであることを特徴とする鍵実装システム。
【請求項3】 記憶部と、LSIとを有する鍵実装システムであって、
前記記憶部は、
最終鍵を、内部鍵を用いて暗号化して得た第1の被暗号化鍵と、
前記内部鍵を、一方向関数による変換によって得た変換鍵を用いて、暗号化して得た第2の被暗号化鍵とを記憶しており、
前記LSIは、
前記記憶部から、前記第1および第2の被暗号化鍵を入力するものであり、かつ、
前記変換鍵の生成元である変換種を生成する種生成部と、
前記種生成部から出力された変換種を、入力された前記

第1の被暗号化鍵を用いて前記一方向関数によって変換し、前記変換鍵を生成する一方向関数回路と、
入力された前記第2の被暗号化鍵を、前記一方向関数回路の出力を鍵として用いて復号化する第1の復号回路と、

入力された前記第1の被暗号化鍵を、前記第1の復号回路の出力を鍵として用いて復号化する第2の復号回路とを備えたものであることを特徴とする鍵実装システム。

【請求項4】 請求項3において、

前記種生成部は、
前記変換種を、記憶するものであることを特徴とする鍵実装システム。

【請求項5】 請求項3において、

前記記憶部は、第1の定数をさらに記憶しており、
前記LSIは、前記記憶部から、前記第1および第2の被暗号化鍵に加えて、前記第1の定数をさらに入力するものであり、
前記種生成部は、

第2の定数を記憶する定数記憶部と、

前記第2の定数を、入力された前記第1の定数を用いて一方向関数によって変換し、前記変換種を生成する第2の一方向関数回路とを備えたものであることを特徴とする鍵実装システム。

【請求項6】 請求項3において、

前記記憶部は、第1の定数を、前記第1の被暗号化鍵を用いて暗号化して得た第3の被暗号化鍵をさらに記憶しており、

前記LSIは、前記記憶部から、前記第1および第2の被暗号化鍵に加えて、前記第3の被暗号化鍵をさらに入力するものであり、
前記種生成部は、

入力された前記第3の被暗号化鍵を、入力された前記第1の被暗号化鍵を鍵として用いて復号化する第3の復号回路と、
前記変換種を、前記第1の定数を用いて暗号化して得た第4の被暗号化鍵を記憶する定数記憶部と、

前記第4の被暗号化鍵を、前記第3の復号回路の出力を鍵として用いて復号化し、前記変換種を生成する第4の復号回路とを備えたものであることを特徴とする鍵実装システム。

【請求項7】 請求項3において、

前記記憶部は、
前記内部鍵を、前記一方向関数による変換によって得たテスト用変換鍵を用いて、暗号化して得た第3の被暗号化鍵をさらに記憶しており、
前記LSIは、

前記記憶部から、前記第1および第2の被暗号化鍵に加えて、前記第3の被暗号化鍵をさらに入力するものであり、かつ、
入力された第2および第3の被暗号化鍵を入力とし、こ

のいずれかを、テスト信号に応じて選択出力する第1のセレクタを備えており、前記第1の復号回路は、前記第2の被暗号化鍵の代わりに、前記第1のセレクタの出力を入力とするものであり、前記種生成部は、前記変換種および、前記テスト用変換鍵の生成元であるテスト用変換種のいずれかを、前記テスト信号に応じて選択出力可能に構成されていることを特徴とする鍵実装システム。

【請求項8】 請求項7において、

前記種生成部は、

前記変換種と、前記テスト用変換種とを記憶する定数記憶部と、

前記変換種およびテスト用変換種を入力とし、そのいずれかを、前記テスト信号に応じて選択出力する第2のセレクタとを備えたものであることを特徴とする鍵実装システム。

【請求項9】 請求項7において、

前記種生成部は、

前記変換種の元になる第1の定数と、前記テスト用変換種の元になる第2の定数とを記憶する第1の定数記憶部と、

前記第1および第2の定数を入力とし、そのいずれかを、前記テスト信号に応じて選択出力する第2のセレクタと、

第3の定数を記憶する第2の定数記憶部と、

前記第3の定数を、前記第2のセレクタの出力を用いて、一方向関数によって変換する第2の一方向関数回路とを備えたものであることを特徴とする鍵実装システム。

【請求項10】 請求項7において、

前記種生成部は、

前記変換種の元になる第1の定数を、前記第1の被暗号化鍵を用いて暗号化して得た第4の被暗号化鍵と、前記テスト用変換鍵の元になる第2の定数を、前記第1の被暗号化鍵を用いて暗号化して得た第5の被暗号化鍵とを記憶する第1の定数記憶部と、

前記第4および第5の被暗号化鍵を入力とし、そのいずれかを、前記テスト信号に応じて選択出力する第2のセレクタと、

前記第2のセレクタの出力を、当該LSIに入力された前記第1の被暗号化鍵を鍵として用いて復号化する第3の復号回路と、

第3の定数を記憶する第2の定数記憶部と、

前記第3の定数を、前記第3の復号回路の出力を用いて、一方向関数によって変換する第2の一方向関数回路とを備えたものであることを特徴とする鍵実装システム。

【請求項11】 請求項8～10のいずれか1項において、

前記LSIは、

前記第2のセレクタの出力を検証する検証回路を備えたものであることを特徴とする鍵実装システム。

【請求項12】 請求項3において、

前記LSIは、

任意の定数が実装可能なヒューズ回路と、

前記第2の復号回路の出力を、前記ヒューズ回路に実装された定数を用いて暗号化し、第3の被暗号化鍵として前記記憶部に出力する暗号回路と、

前記記憶部から入力された第3の被暗号化鍵を、前記ヒューズ回路に実装された定数を用いて復号する第3の復号回路とを備えたものであり、

前記記憶部は、

前記LSIから前記第3の被暗号化鍵を受けたとき、前記第1および第2の被暗号化鍵を消去してこの第3の被暗号化鍵を記憶とともに、前記LSIに前記第3の被暗号化鍵を出力するものであることを特徴とする鍵実装システム。

【請求項13】 請求項3において、

前記LSIは、

任意の定数が実装可能なヒューズ回路と、

前記ヒューズ回路に実装された定数を、前記種生成部から出力された変換種を用いて、一方向関数によって変換する第2の一方向関数回路と、

前記第2の復号回路の出力を、前記第2の一方向関数回路の出力を用いて暗号化し、第3の被暗号化鍵として前記記憶部に出力する暗号回路と、

前記記憶部から入力された第3の被暗号化鍵を、前記第2の一方向関数回路の出力を用いて復号化する第3の復号回路とを備えたものであり、

前記記憶部は、

前記LSIから前記第3の被暗号化鍵を受けたとき、前記第1および第2の被暗号化鍵を消去して、この第3の被暗号化鍵を記憶とともに、前記LSIに前記第3の被暗号化鍵を出力することを特徴とする鍵実装システム。

【請求項14】 請求項13において、

前記LSIは、

前記記憶部から入力された第3の被暗号化鍵と、前記暗号回路の出力を入力とし、このいずれかをテスト信号に応じて選択出力するセレクタを備え、

前記第3の復号回路は、前記記憶部から入力された第3の被暗号化鍵の代わりに、前記セレクタの出力を入力とするものであることを特徴とする鍵実装システム。

【請求項15】 鍵実装システムを実現するためのLSIであって、

最終鍵を、第1の内部鍵を用いて暗号化して得た第1の被暗号化鍵を第1の入力とし、第2の内部鍵を、前記第1の被暗号化鍵を用いて暗号化して得た第2の被暗号化鍵を第2の入力としたとき、前記最終鍵を生成可能に構

成されており、

前記第1の内部鍵を、前記第2の内部鍵を用いて暗号化して得た第3の被暗号化鍵を記憶する記憶部と、
前記第2の入力を、前記第1の入力を鍵として用いて復号化する第1の復号回路と、
前記第3の被暗号化鍵を、前記第1の復号回路の出力を鍵として用いて復号化する第2の復号回路と、
前記第1の入力を、前記第2の復号回路の出力を鍵として用いて復号化する第3の復号回路とを備えたものであることを特徴とするLSI。

【請求項16】 鍵実装システムを実現するためのLSIであって、

最終鍵を、内部鍵を用いて暗号化して得た第1の被暗号化鍵を第1の入力とし、前記内部鍵を、一方向関数による変換によって得た変換鍵を用いて、暗号化して得た第2の被暗号化鍵を、第2の入力としたとき、前記最終鍵を生成可能に構成されており、

前記変換鍵の生成元である変換種を生成する種生成部と、

前記種生成部から出力された変換種を、前記第1の入力を用いて前記一方向関数によって変換し、前記変換鍵を生成する一方向関数回路と、

前記第2の入力を、前記一方向関数回路の出力を鍵として用いて復号化する第1の復号回路と、

前記第1の入力を、前記第1の復号回路の出力を鍵として用いて復号化する第2の復号回路とを備えたものであることを特徴とするLSI。

【請求項17】 請求項16において、

任意の定数が実装可能なヒューズ回路と、

前記第2の復号回路の出力を、前記ヒューズ回路に実装された定数を用いて暗号化し、第3の被暗号化鍵として当該LSI外部に出力する暗号回路と、

当該LSIの第3の入力を、前記ヒューズ回路に実装された定数を用いて復号する第3の復号回路とを備えたことを特徴とするLSI。

【請求項18】 請求項16において、

任意の定数が実装可能なヒューズ回路と、

前記ヒューズ回路に実装された定数を、前記種生成部から出力された変換種を用いて、一方向関数によって変換する第2の一方向関数回路と、

前記第2の復号回路の出力を、前記第2の一方向関数回路の出力を用いて暗号化し、第3の被暗号化鍵として当該LSI外部に出力する暗号回路と、

第3の入力を、前記第2の一方向関数回路の出力を用いて復号化する第3の復号回路とを備えたことを特徴とするLSI。

【請求項19】 システムに、鍵を実装する方法であって、

前記システムが有する記憶部に、最終鍵を、第1の内部鍵を用いて暗号化して得た第1の被暗号化鍵と、第2の

内部鍵を、前記第1の被暗号化鍵を用いて暗号化して得た第2の被暗号化鍵とを記憶させる工程と、

前記システムに、LSIを実装する工程とを備え、
前記LSIは、

前記第1の内部鍵を、前記第2の内部鍵を用いて暗号化して得た第3の被暗号化鍵を記憶しており、前記記憶部から、前記第1および第2の被暗号化鍵を入力するものであり、かつ、

入力された第2の被暗号化鍵を、入力された第1の被暗号化鍵を鍵として用いて復号化する第1の復号回路と、前記第3の被暗号化鍵を、前記第1の復号回路の出力を鍵として用いて復号化する第2の復号回路と、

入力された第1の被暗号化鍵を、前記第2の復号回路の出力を鍵として用いて復号化する第3の復号回路とを備えたものであることを特徴とする鍵実装方法。

【請求項20】 システムに、鍵を実装する方法であって、
前記システムが有する記憶部に、最終鍵を、内部鍵を用いて暗号化して得た第1の被暗号化鍵と、前記内部鍵を、一方向関数による変換によって得た変換鍵を用いて暗号化して得た第2の被暗号化鍵とを記憶させる工程と、

前記システムに、LSIを実装する工程とを備え、
前記LSIは、

前記記憶部から、前記第1および第2の被暗号化鍵を入力するものであり、かつ、

前記変換鍵の生成元である変換種を生成する種生成部と、

前記種生成部から出力された変換種を、入力された前記第1の被暗号化鍵を用いて前記一方向関数によって変換し、前記変換鍵を生成する一方向関数回路と、入力された前記第2の被暗号化鍵を、前記一方向関数回路の出力を鍵として用いて復号化する第1の復号回路と、

入力された前記第1の被暗号化鍵を、前記第1の復号回路の出力を鍵として用いて復号化する第2の復号回路とを備えたものであることを特徴とする鍵実装方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、鍵が実装されたシステムやこれに用いるLSIに関する技術に属する。

【0002】

【従来の技術】従来の鍵実装システムでは、通常、値が固定された生の鍵を、LSI内に実装していた。

【0003】

【発明が解決しようとする課題】通常のCMOSLSIの内部では、LSIの個体毎に違う鍵を実装するのは困難である。すなわち、LSI内部に閉じた鍵を変更する手段がない。また、外部ROM等からのロードでは、システム（セット）上で解析が可能となる。また、鍵管理者以外に、LSI設計者またはシステム（セット）設計

者等が鍵を知るおそれがある。また、違った値の鍵を大量生産技術によって書き込みにくい。また、鍵実装が正確に行われたか否かを検証することができない。すなわち、内部鍵のテストが困難である。

【0004】前記の問題に鑑み、本発明は、鍵実装システムとして、鍵の機密性および秘匿性をより向上させることを課題とする。

【0005】また、本発明は、様々な機密鍵を容易に実装することが可能なLSIを提供することを課題とする。

【0006】さらに、本発明は、鍵実装システムとして、回路規模を増大させることなく、実装された値のテストを可能にすることを課題とする。

【0007】

【課題を解決するための手段】前記の課題を解決するために、請求項1の発明が講じた解決手段は、記憶部とLSIとを有する鍵実装システムであって、前記記憶部は、最終鍵を第1の内部鍵を用いて暗号化して得た第1の被暗号化鍵と、第2の内部鍵を前記第1の被暗号化鍵を用いて暗号化して得た第2の被暗号化鍵とを記憶しており、前記LSIは、前記第1の内部鍵を前記第2の内部鍵を用いて暗号化して得た第3の被暗号化鍵を記憶しており、前記記憶部から前記第1および第2の被暗号化鍵を入力するものであり、かつ、入力された第2の被暗号化鍵を入力された第1の被暗号化鍵を鍵として用いて復号化する第1の復号回路と、前記第3の被暗号化鍵を前記第1の復号回路の出力を鍵として用いて復号化する第2の復号回路と、入力された第1の被暗号化鍵を前記第2の復号回路の出力を鍵として用いて復号化する第3の復号回路とを備えたものである。

【0008】請求項1の発明によると、LSIにおいて、第1の復号回路によって、記憶部に記憶された第2の被暗号化鍵が、記憶部に記憶された第1の被暗号化鍵を鍵として復号化されて第2の内部鍵が生成され、第2の復号回路によって、LSIに記憶された第3の被暗号化鍵が、第1の復号回路の出力すなわち第2の内部鍵を鍵として復号化されて第1の内部鍵が生成される。さらに、第3の復号回路によって、第1の被暗号化鍵が、第2の復号回路の出力すなわち第1の内部鍵を鍵として復号化されて最終鍵が生成される。すなわち、記憶部およびLSIに実装された鍵は、全て、暗号化されたものであり、しかも、LSIで最終鍵が生成される。このため、システム上において、鍵の解析が困難になり、機密性が向上する。また、生の機密鍵を開発者や実装者に見えなくとも、LSIおよびシステムの開発および実装が可能になる。

【0009】請求項2の発明では、前記請求項1の鍵実装システムにおけるLSIは、第1のテスト用内部鍵を第2のテスト用内部鍵を用いて暗号化して得た第4の被暗号化鍵をさらに記憶しており、かつ、前記第3および

第4の被暗号化鍵を入力とし、このいずれかを第1のテスト信号に応じて選択出力する第1のセレクタと、前記第1のセレクタの選択出力と前記第2の復号回路の出力を入力とし、このいずれかを第2のテスト信号に応じて選択出力する第2のセレクタとを備えたものとし、前記第2の復号回路は、前記第3の被暗号化鍵の代わりに前記第1のセレクタの出力を入力とするものとし、前記第3の復号回路は、前記第2の復号回路の出力の代わりに前記第2のセレクタの出力を鍵として入力するものとする。

【0010】請求項2の発明によると、まず、第1のセレクタは第4の被暗号化鍵を選択し、第2のセレクタは第2の復号回路の出力を選択するよう、第1および第2のテスト信号を設定する。このとき、第1の復号回路に、テスト用最終鍵を第1のテスト用内部鍵を鍵として用いて暗号化して得た開発用被暗号化鍵を、鍵として与えるとともに、この開発用被暗号化鍵を鍵として用いて第2のテスト用内部鍵を暗号化して得た被暗号化鍵を、復号化の対象として与える。これにより、第1の復号回路から第2のテスト用内部鍵が生成され、第2の復号回路から第1のテスト用内部鍵が生成される。そして、第3の復号回路に、前記開発用被暗号化鍵を復号化の対象として与えることによって、テスト用最終鍵が生成される。すなわち、実際の最終鍵を生成することなく、第1～第3の復号回路が正常に動作するか否かをテストすることができる。

【0011】また、第1のセレクタは第3の被暗号化鍵を選択し、第2のセレクタは第1のセレクタの出力すなわち第3の被暗号化鍵を選択するよう、第1および第2のテスト信号を設定する。このとき、第3の復号回路に、第3の被暗号化鍵を鍵として用いてテスト用最終鍵を暗号化して得た被暗号化鍵を、復号化の対象として与える。この被暗号化鍵は第3の復号回路によって、第3の被暗号化鍵を鍵として復号化され、これにより、テスト用最終鍵が生成される。すなわち、実際の最終鍵を生成することなく、第3の被暗号化鍵が正しく実装されているか否かをテストすることができる。

【0012】また、請求項3の発明が講じた解決手段は、記憶部とLSIとを有する鍵実装システムとして、前記記憶部は、最終鍵を内部鍵を用いて暗号化して得た第1の被暗号化鍵と、前記内部鍵を一方向関数による変換によって得た変換鍵を用いて暗号化して得た第2の被暗号化鍵とを記憶しており、前記LSIは、前記記憶部から、前記第1および第2の被暗号化鍵を入力するものであり、かつ、前記変換鍵の生成元である変換種を生成する種生成部と、前記種生成部から出力された変換種を入力された前記第1の被暗号化鍵を用いて前記一方向関数によって変換し、前記変換鍵を生成する一方向関数回路と、入力された前記第2の被暗号化鍵を前記一方向関数回路の出力を鍵として用いて復号化する第1の復号回

路と、入力された前記第1の被暗号化鍵を前記第1の復号回路の出力を鍵として用いて復号化する第2の復号回路とを備えたものである。

【0013】請求項3の発明によると、LSIにおいて、一方向関数回路によって、種生成部から生成された変換種は第1の被暗号化鍵を用いて変換され、変換鍵が生成される。そして第1の復号回路によって、第2の被暗号化鍵が変換鍵を鍵として用いて復号化されて内部鍵が生成され、第2の復号回路によって、第1の被暗号化鍵が内部鍵を鍵として復号されて最終鍵が生成される。ここで、内部鍵を異なる値に変更するとき、第1の被暗号化鍵を新たに生成し、同一の変換種を用いて一方向関数によって新たな変換鍵を生成し、さらに第2の被暗号化鍵を新たに生成すればよい。すなわち、変換種を変えることなく、内部鍵や第1および第2の被暗号化鍵を任意に設定することができるので、共通のLSIを用いて、システム毎に個別に、暗号化する鍵を設定することができる。

【0014】そして、請求項4の発明では、前記請求項3の鍵実装システムにおける種生成部は、前記変換種を記憶するものとする。

【0015】また、請求項5の発明では、前記請求項3の鍵実装システムにおいて、前記記憶部は第1の定数をさらに記憶しており、前記LSIは、前記記憶部から、前記第1および第2の被暗号化鍵に加えて前記第1の定数をさらに入力するものであり、前記種生成部は、第2の定数を記憶する定数記憶部と、前記第2の定数を入力された前記第1の定数を用いて一方向関数によって変換し、前記変換種を生成する第2の一方向関数回路とを備えたものとする。

【0016】また、請求項6の発明では、前記請求項3の鍵実装システムにおいて、前記記憶部は、第1の定数を前記第1の被暗号化鍵を用いて暗号化して得た第3の被暗号化鍵をさらに記憶しており、前記LSIは、前記記憶部から、前記第1および第2の被暗号化鍵に加えて前記第3の被暗号化鍵をさらに入力するものであり、前記種生成部は、入力された前記第3の被暗号化鍵を入力された前記第1の被暗号化鍵を鍵として用いて復号化する第3の復号回路と、前記変換種を前記第1の定数を用いて暗号化して得た第4の被暗号化鍵を記憶する定数記憶部と、前記第4の被暗号化鍵を前記第3の復号回路の出力を鍵として用いて復号化し、前記変換種を生成する第4の復号回路とを備えたものとする。

【0017】また、請求項7の発明では、前記請求項3の鍵実装システムにおいて、前記記憶部は、前記内部鍵を、前記一方向関数による変換によって得たテスト用変換鍵を用いて暗号化して得た第3の被暗号化鍵をさらに記憶しており、前記LSIは、前記記憶部から、前記第1および第2の被暗号化鍵に加えて前記第3の被暗号化鍵をさらに入力するものであり、かつ、入力された第2

および第3の被暗号化鍵を入力とし、このいずれかをテスト信号に応じて選択出力する第1のセレクタを備えており、前記第1の復号回路は、前記第2の被暗号化鍵の代わりに前記第1のセレクタの出力を入力とするものであり、前記種生成部は、前記変換種および、前記テスト用変換鍵の生成元であるテスト用変換種のいずれかを、前記テスト信号に応じて選択出力可能に構成されているものとする。

【0018】そして、請求項8の発明では、前記請求項7の鍵実装システムにおける種生成部は、前記変換種と前記テスト用変換種とを記憶する定数記憶部と、前記変換種およびテスト用変換種を入力とし、そのいずれかを前記テスト信号に応じて選択出力する第2のセレクタとを備えたものとする。

【0019】また、請求項9の発明では、前記請求項7の鍵実装システムにおける種生成部は、前記変換種の元になる第1の定数と前記テスト用変換種の元になる第2の定数とを記憶する第1の定数記憶部と、前記第1および第2の定数を入力とし、そのいずれかを前記テスト信号に応じて選択出力する第2のセレクタと、第3の定数を記憶する第2の定数記憶部と、前記第3の定数を、前記第2のセレクタの出力を用いて一方向関数によって変換する第2の一方向関数回路とを備えたものとする。

【0020】また、請求項10の発明では、前記請求項7の鍵実装システムにおける種生成部は、前記変換種の元になる第1の定数を前記第1の被暗号化鍵を用いて暗号化して得た第4の被暗号化鍵と、前記テスト用変換鍵の元になる第2の定数を前記第1の被暗号化鍵を用いて暗号化して得た第5の被暗号化鍵とを記憶する第1の定数記憶部と、前記第4および第5の被暗号化鍵を入力とし、そのいずれかを前記テスト信号に応じて選択出力する第2のセレクタと、前記第2のセレクタの出力を当該LSIに入力された前記第1の被暗号化鍵を鍵として用いて復号化する第3の復号回路と、第3の定数を記憶する第2の定数記憶部と、前記第3の定数を、前記第3の復号回路の出力を用いて一方向関数によって変換する第2の一方向関数回路とを備えたものとする。

【0021】そして、請求項11の発明では、前記請求項8～10のいずれか1項におけるLSIは、前記第2のセレクタの出力を検証する検証回路を備えたものとする。

【0022】また、請求項12の発明では、前記請求項3の鍵実装システムにおいて、前記LSIは、任意の定数が実装可能なヒューズ回路と、前記第2の復号回路の出力を前記ヒューズ回路に実装された定数を用いて暗号化し、第3の被暗号化鍵として前記記憶部に出力する暗号回路と、前記記憶部から入力された第3の被暗号化鍵を前記ヒューズ回路に実装された定数を用いて復号する第3の復号回路とを備えたものとし、前記記憶部は、前記LSIから前記第3の被暗号化鍵を受けたとき、前記

第1および第2の被暗号化鍵を消去してこの第3の被暗号化鍵を記憶するともに前記LSIに前記第3の被暗号化鍵を出力するものとする。

【0023】また、請求項13の発明では、前記請求項3の鍵実装システムにおいて、前記LSIは、任意の定数が実装可能なヒューズ回路と、前記ヒューズ回路に実装された定数を、前記種生成部から出力された変換種を用いて一方向関数によって変換する第2の一方向関数回路と、前記第2の復号回路の出力を前記第2の一方向関数回路の出力を用いて暗号化し、第3の被暗号化鍵として前記記憶部に出力する暗号回路と、前記記憶部から入力された第3の被暗号化鍵を前記第2の一方向関数回路の出力を用いて復号化する第3の復号回路とを備えたものとし、前記記憶部は、前記LSIから前記第3の被暗号化鍵を受けたとき、前記第1および第2の被暗号化鍵を消去してこの第3の被暗号化鍵を記憶するともに、前記LSIに前記第3の被暗号化鍵を出力するものとする。

【0024】そして、請求項14の発明では、前記請求項13の鍵実装システムにおいて、前記LSIは、前記記憶部から入力された第3の被暗号化鍵と前記暗号回路の出力をと入力とし、このいずれかをテスト信号に応じて選択出力するセレクタを備え、前記第3の復号回路は、前記記憶部から入力された第3の被暗号化鍵の代わりに前記セレクタの出力を入力とするものとする。

【0025】また、請求項15の発明が講じた解決手段は、鍵実装システムを実現するためのLSIとして、最終鍵を第1の内部鍵を用いて暗号化して得た第1の被暗号化鍵を第1の入力とし、第2の内部鍵を前記第1の被暗号化鍵を用いて暗号化して得た第2の被暗号化鍵を第2の入力としたとき、前記最終鍵を生成可能に構成されており、前記第1の内部鍵を前記第2の内部鍵を用いて暗号化して得た第3の被暗号化鍵を記憶する記憶部と、前記第2の入力を前記第1の入力を鍵として用いて復号化する第1の復号回路と、前記第3の被暗号化鍵を前記第1の復号回路の出力を鍵として用いて復号化する第2の復号回路と、前記第1の入力を前記第2の復号回路の出力を鍵として用いて復号化する第3の復号回路とを備えたものである。

【0026】また、請求項16の発明が講じた解決手段は、鍵実装システムを実現するためのLSIとして、最終鍵を内部鍵を用いて暗号化して得た第1の被暗号化鍵を第1の入力とし、前記内部鍵を一方向関数による変換によって得た変換鍵を用いて暗号化して得た第2の被暗号化鍵を第2の入力としたとき、前記最終鍵を生成可能に構成されており、前記変換鍵の生成元である変換種を生成する種生成部と、前記種生成部から出力された変換種を前記第1の入力を用いて前記一方向関数によって変換し、前記変換鍵を生成する一方向関数回路と、前記第2の入力を前記一方向関数回路の出力を鍵として用い

て復号化する第1の復号回路と、前記第1の入力を前記第1の復号回路の出力を鍵として用いて復号化する第2の復号回路とを備えたものである。

【0027】そして、請求項17の発明では、前記請求項16のLSIは、任意の定数が実装可能なヒューズ回路と、前記第2の復号回路の出力を前記ヒューズ回路に実装された定数を用いて暗号化し、第3の被暗号化鍵として当該LSI外部に出力する暗号回路と、当該LSIの第3の入力を、前記ヒューズ回路に実装された定数を用いて復号する第3の復号回路とを備えたものとする。

【0028】また、請求項18の発明では、前記請求項16のLSIは、任意の定数が実装可能なヒューズ回路と、前記ヒューズ回路に実装された定数を前記種生成部から出力された変換種を用いて一方向関数によって変換する第2の一方向関数回路と、前記第2の復号回路の出力を前記第2の一方向関数回路の出力を用いて暗号化し、第3の被暗号化鍵として当該LSI外部に出力する暗号回路と、第3の入力を前記第2の一方向関数回路の出力を用いて復号化する第3の復号回路とを備えたものとする。

【0029】また、請求項19の発明が講じた解決手段は、システムに鍵を実装する方法として、前記システムが有する記憶部に、最終鍵を、第1の内部鍵を用いて暗号化して得た第1の被暗号化鍵と、第2の内部鍵を、前記第1の被暗号化鍵を用いて暗号化して得た第2の被暗号化鍵とを記憶させる工程と、前記システムにLSIを実装する工程とを備え、前記LSIは、前記第1の内部鍵を、前記第2の内部鍵を用いて暗号化して得た第3の被暗号化鍵を記憶しており、前記記憶部から、前記第1および第2の被暗号化鍵を入力するものであり、かつ、入力された第2の被暗号化鍵を、入力された第1の被暗号化鍵を鍵として用いて復号化する第1の復号回路と、前記第3の被暗号化鍵を、前記第1の復号回路の出力を鍵として用いて復号化する第2の復号回路と、入力された第1の被暗号化鍵を、前記第2の復号回路の出力を鍵として用いて復号化する第3の復号回路とを備えたものである。

【0030】また、請求項20の発明が講じた解決手段は、システムに鍵を実装する方法として、前記システムが有する記憶部に、最終鍵を、内部鍵を用いて暗号化して得た第1の被暗号化鍵と、前記内部鍵を、一方向関数による変換によって得た変換鍵を用いて暗号化して得た第2の被暗号化鍵とを記憶させる工程と、前記システムにLSIを実装する工程とを備え、前記LSIは、前記記憶部から、前記第1および第2の被暗号化鍵を入力するものであり、かつ、前記変換鍵の生成元である変換種を生成する種生成部と、前記種生成部から出力された変換種を、入力された前記第1の被暗号化鍵を用いて前記一方向関数によって変換し、前記変換鍵を生成する一方向関数回路と、入力された前記第2の被暗号化鍵を、前

記一方向関数回路の出力を鍵として用いて復号化する第1の復号回路と、入力された前記第1の被暗号化鍵を、前記第1の復号回路の出力を鍵として用いて復号化する第2の復号回路とを備えたものである。

【0031】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照して説明する。

【0032】なお、以下の説明において、暗号および復号の処理については、対称暗号を前提とする。「対称暗号」とは、図20に示すように、Aを入力としてBを鍵として用いて暗号化して得た被暗号化鍵をCとすると、Cを入力としてBを鍵として復号化したものは、Aとなる特性を持つものである。

【0033】また、Xを鍵Yを用いて暗号化して得た被暗号化鍵のことを、EX(Y)と表現するものとする。

【0034】(第1の実施形態)図1は本発明の第1の実施形態に係る鍵実装システムの構成を示す図である。図1において、本実施形態に係る鍵実装システム1は、記憶部1aとLSI10とを備えている。記憶部1aは、最終鍵DK1を、第1の内部鍵MK1を用いて暗号化して得た第1の被暗号化鍵EDK1(MK1)と、第2の内部鍵KEY1を、第1の被暗号化鍵EDK1(MK1)を用いて暗号化して得た第2の被暗号化鍵EKEY1(EDK1(MK1))とを、記憶している。

【0035】LSI10は、第1の内部鍵MK1を、第2の内部鍵KEY1を用いて暗号化して得た第3の被暗号化鍵EMK1(KEY1)を鍵記憶部11に記憶している。また、第2の入力IN2を、第1の入力IN1を鍵として用いて復号化する第1の復号回路12と、鍵記憶部11に記憶された第3の被暗号化鍵EMK1(KEY1)を、第1の復号回路12の出力を鍵として用いて復号化する第2の復号回路13と、第1の入力IN1を、第2の復号回路13の出力を鍵として用いて復号化する第3の復号回路14とを備えている。

【0036】LSI10が鍵実装システム1に実装されると、記憶部1aに記憶された第1および第2の被暗号化鍵EDK1(MK1), EKEY1(EDK1(MK1))が、それぞれ、第1および第2の入力IN1, IN2としてLSI10に入力される。

【0037】このとき、LSI10は次のように動作する。すなわち、第1の復号回路12は、第2の入力IN2すなわち第2の被暗号化鍵EKEY1(EDK1(MK1))を、第1の入力IN1すなわち第1の被暗号化鍵EDK1(MK1)を鍵として用いて復号化する。これにより、第1の復号回路12から、第2の内部鍵KEY1が outputされる。第2の復号回路13は、鍵記憶部11に記憶された第3の被暗号化鍵EMK1(KEY1)を、第1の復号回路12の出力すなわち第2の内部鍵KEY1を鍵として用いて復号化する。これにより、第2の復号回路13から、第1の内部鍵MK1が出力され

る。そして、第3の復号回路14は、第1の入力IN1すなわち第1の被暗号化鍵EDK1(MK1)を、第2の復号回路13の出力すなわち第1の内部鍵MK1を鍵として用いて復号化する。これにより、第3の復号回路14から、最終鍵DK1が出力される。

【0038】このように、第1および第2の被暗号化鍵EDK1(MK1), EKEY1(EDK1(MK1))を記憶する記憶部1aと、第3の被暗号化鍵EMK1(KEY1)を記憶するLSI10とを組み合わせて実装することによって、最終鍵DK1が生成される鍵実装システム1を実現することができる。そして、記憶部1aおよびLSI10では、機密鍵が全て暗号化して実装されているので、システム上での解析も困難であり、機密性が高い。

【0039】また、開発過程においても、生の鍵が存在しないので、開発段階での秘匿性も大幅に向上する。

【0040】図2は図1における各被暗号化鍵を生成する鍵生成の手順の一例を示す図である。図2に示すように、鍵管理者は、最終鍵DK1を、任意の第1の内部鍵MK1を鍵として用いて暗号化し、第1の被暗号化鍵EDK1(MK1)を生成する(S11)。次に、第1の内部鍵MK1を、任意の第2の内部鍵KEY1を鍵として用いて暗号化し、第3の被暗号化鍵EMK1(KEY1)を生成する(S12)。さらに、第2の内部鍵KEY1を、第1の被暗号化鍵EDK1(MK1)を鍵として用いて暗号化し、第2の被暗号化鍵EKEY1(EDK1(MK1))を生成する(S13)。

【0041】そして、鍵管理者は、第1および第2の被暗号化鍵EDK1(MK1), EKEY1(EDK1(MK1))を機器実装者すなわちシステム1の開発者に提供するとともに、第3の被暗号化鍵EMK1(KEY1)をLSI10の開発者に提供する。このように鍵を生成することによって、開発者に、最終鍵DK1や第1および第2の内部鍵MK1, KEY1を提供する必要が生じないので、開発段階での鍵の秘匿性も大幅に向上する。

【0042】システム1の製造時には、記憶部1aに、第1および第2の被暗号化鍵EDK1(MK1), EKEY1(EDK1(MK1))を記憶させるとともに、LSI10を実装する。

【0043】(第2の実施形態)図3は本発明の第2の実施形態に係る鍵実装システムの構成を示す図である。図3において、図1と共通の構成要素には、図1と同一の符号を付している。

【0044】LSI20において、鍵記憶部11Aは、第3の被暗号化鍵EMK1(KEY1)に加えて、第1のテスト用内部鍵tstMK1を、第2のテスト用内部鍵tstKEY1を用いて暗号化して得た第4の被暗号化鍵E tst MK1(tstKEY1)をさらに記憶している。

【0045】また、LSI20には、第1および第2のセレクタ15、16が新たに設けられている。セレクタ15、16はともに、選択信号が“1”的ときは入力Aを選択する一方、選択信号が“0”的ときは入力Bを選択する。第1のセレクタ15は、鍵記憶部11Aに記憶された第3および第4の被暗号化鍵EMK1(KEY1)、EtstMK1(tstKEY1)を入力とし、このいずれかを、第1のテスト信号TAに応じて選択出力する。第2の復号回路13は、第1のセレクタ15の出力を入力とする。また、第2のセレクタ16は、第1のセレクタ15の出力と第2の復号回路13の出力を入力とし、このいずれかを、第2のテスト信号TBに応じて選択出力する。第3の復号回路14は、第2のセレクタ16の出力を鍵として入力する。

【0046】ここで、第1および第2のテスト信号TA、TBをともに“0”に設定する。すなわち、第1および第2のセレクタ15、16は、ともに、入力Bを選択出力する。これにより、システム2におけるLSI20の通常動作が実現される。

【0047】すなわち、第1の実施形態と同様に、記憶部1aからLSI20に、第1の被暗号化鍵EDK1(MK1)が第1の入力IN1として、第2の被暗号化鍵EKEY1(EDK1(MK1))が第2の入力IN2として、それぞれ入力される。第1の復号回路12は、入力された第2の被暗号化鍵EKEY1(EDK1(MK1))を、入力された第1の被暗号化鍵EDK1(MK1)を鍵として用いて復号化し、第2の内部鍵KEY1を生成する。

【0048】第1のセレクタ15は、第1のテスト信号TAが“0”であるので、入力Bすなわち第3の被暗号化鍵EMK1(KEY1)を選択出力する。第2の復号回路13は、第1のセレクタ15の出力すなわち第3の被暗号化鍵EMK1(KEY1)を、第2の復号回路12の出力すなわち第2の内部鍵KEY1を鍵として用いて復号化し、第1の内部鍵MK1を生成する。

【0049】第2のセレクタ16は、第2のテスト信号TBが“0”であるので、入力Bすなわち、第2の復号回路13の出力すなわち第1の内部鍵MK1を選択出力する。第3の復号回路14は、入力された第1の被暗号化鍵EDK1(MK1)を、第1の内部鍵MK1を鍵として用いて復号化し、最終鍵DK1を生成する。すなわち、第1の実施形態と同様の動作が実行される。

【0050】図3において、第1および第2のテスト信号TA、TBがともに“0”であるとき以外の場合は、最終鍵DK1は正常に生成されない。例えばいま、第1および第2のテスト信号TA、TBはともに“1”に設定されているものとする。

【0051】第1のセレクタ15は第1のテスト信号TAを受けて、入力Aすなわち第4の被暗号化鍵EtstMK1(tstKEY1)を選択出力する。また第2の

セレクタ16は第2のテスト信号TBを受けて、入力Aすなわち、第1のセレクタ15の出力すなわち第4の被暗号化鍵EtstMK1(tstKEY1)を選択出力する。このとき、第3の復号回路14は、入力された第1の被暗号化鍵EDK1(MK1)を、第2のセレクタ16の出力すなわち第4の被暗号化鍵EtstMK1(tstKEY1)を鍵として復号化する。この結果、第3の復号回路14から最終鍵DK1が生成されることはない。

【0052】図4は本実施形態に係るLSI20の開発時におけるテストベンチの構成を示す図である。図4において、テストベンチ2Bに設けられたテスト記憶部2bには、LSI開発用の被暗号化鍵が実装されている。このため、LSI開発時には、製品用の鍵を見ることなく開発することができる。

【0053】すなわち、テスト記憶部2bは、鍵tstDK1を第3の被暗号化鍵EMK1(KEY1)を用いて暗号化して得た第1の開発用被暗号化鍵EtstDK1(EMK1(KEY1))と、鍵tstDK1を鍵tstMK1を用いて暗号化して得た第2の開発用被暗号化鍵EtstDK1(tstMK1)と、第2の開発用被暗号化鍵EtstDK1(tstMK1)を用いて鍵tstKEY1を暗号化して得た第3の開発用被暗号化鍵EtstKEY1(EtstDK1(tstMK1))とを、記憶している。ここで、鍵tstDK1、tstMK1、tstKEY1はいずれも開発用の鍵であり、実際の製品(システム)上では使用されないものとする。

【0054】また、テストベンチ2Bには、第3のセレクタ17が設けられている。第3のセレクタ17は、第1の開発用被暗号化鍵EtstDK1(EMK1(KEY1))を入力A、第2の開発用被暗号化鍵EtstDK1(tstMK1)を入力Bとし、このいずれかを、第2のテスト信号TBに応じて選択出力する。第3のセレクタ17の出力は、第1の入力IN1としてLSI20に入力される。

【0055】図4において、まず、第1～第3の復号回路12、13、14が正常に動作するか否かをテストする。この場合、第1のテスト信号TAを“1”に設定するとともに、第2のテスト信号TBを“0”に設定する。

【0056】このとき、第3のセレクタ17は第2のテスト信号TBを受けて、入力Bすなわち第2の開発用被暗号化鍵EtstDK1(tstMK1)を選択出力する。第1の復号回路12は、入力IN2として入力された第3の開発用被暗号化鍵EtstKEY1(EtstDK1(tstMK1))を、第2の開発用被暗号化鍵EtstDK1(tstMK1)を鍵として用いて復号化し、第2のテスト用内部鍵tstKEY1を生成する。

【0057】第1のセレクタ15は第1のテスト信号TAを受けて、入力Aすなわち第4の被暗号化鍵ESTMK1(tstKEY1)を選択出力する。第2の復号回路13は、第2のセレクタ15の出力すなわち第4の被暗号化鍵ESTMK1(tstKEY1)を、第1の復号回路12の出力すなわち第2のテスト用内部鍵tstKEY1を鍵として用いて復号化し、第1のテスト用内部鍵tstMK1を生成する。第2のセレクタ16は第2のテスト信号TBを受けて、入力Bすなわち、第2の復号回路13の出力すなわち第1のテスト用内部鍵tstMK1を選択出力する。第3の復号回路14は、入力IN1すなわち第2の開発用被暗号化鍵ESTDK1(tstMK1)を、第2のセレクタ16の出力すなわち第1のテスト用内部鍵tstMK1を鍵として用いて復号化し、テスト用最終鍵tstDK1を生成する。

【0058】次に、実際の製品に使用される第3の被暗号化鍵EMK1(KEY1)が正しく実装されているか否かをテストする。この場合、第1のテスト信号TAを“0”に設定するとともに、第2のテスト信号TBを“1”に設定する。

【0059】このとき、第3のセレクタ17は第2のテスト信号TBを受けて、入力Aすなわち第1の開発用被暗号化鍵ESTDK1(EMK1(KEY1))を選択出力する。この第1の開発用被暗号化鍵ESTDK1(EMK1(KEY1))は、第3の復号回路14に入力として与えられる。

【0060】第1のセレクタ15は第1のテスト信号TAを受けて、入力Bすなわち第3の被暗号化鍵EMK1(KEY1)を選択出力する。第2のセレクタ16は第2のテスト信号TBを受けて、入力Aすなわち、第1のセレクタ15の出力すなわち第3の被暗号化鍵EMK1(KEY1)を選択出力する。第3の復号回路14は、第1の開発用被暗号化鍵ESTDK1(EMK1(KEY1))を、第3の被暗号化鍵EMK1(KEY1)を鍵として用いて復号化し、テスト用最終鍵tstDK1を生成する。すなわち、テスト用最終鍵tstDK1が正常に生成されるか否かによって、第3の被暗号化鍵EMK1(KEY1)が正しく実装されているか否かを判断することができる。

【0061】図5は図3および図4における各被暗号化鍵を生成する鍵生成の手順の一例を示す図である。図5に示すように、鍵管理者は、最終鍵DK1を、任意の第1の内部鍵MK1を鍵として用いて暗号化し、第1の被暗号化鍵EDK1(MK1)を生成する(S11)。次に、第1の内部鍵MK1を、任意の第2の内部鍵KEY1を鍵として用いて暗号化し、第3の被暗号化鍵EMK1(KEY1)を生成する(S12)。さらに、第2の内部鍵KEY1を、第1の被暗号化鍵EDK1(MK1)を鍵として用いて暗号化し、第2の被暗号化鍵EK

EY1(EDK1(MK1))を生成する(S13)。

【0062】そして、鍵管理者は、第1および第2の被暗号化鍵EDK1(MK1), EKEY1(EDK1(MK1))を機器実装者に提供するとともに、第3の被暗号化鍵EMK1(KEY1)をLSI20の開発者に提供する。ここまででは、図2の手順と同様である。

【0063】これとともに、鍵管理者は、テスト用最終鍵tstDK1を、任意の第1のテスト用内部鍵tstMK1を用いて暗号化し、第2の開発用被暗号化鍵ESTDK1(tstMK1)を生成する(S21)。次に、第1のテスト用内部鍵tstMK1を、任意の第2のテスト用内部鍵tstKEY1を用いて暗号化し、第4の被暗号化鍵ESTDK1(tstKEY1)を生成する(S22)。さらに、第2のテスト用内部鍵tstKEY1を、第2の開発用被暗号化鍵ESTDK1(tstMK1)を用いて暗号化し、第3の開発用被暗号化鍵ESTDK1(tstEDK1(tstMK1))を生成する(S23)。そして、テスト用最終鍵tstDK1を、第3の被暗号化鍵EMK1(KEY1)を用いて暗号化し、第1の開発用被暗号化鍵ESTDK1(EMK1(KEY1))を生成する(S24)。

【0064】そして、鍵管理者は、第4の被暗号化鍵ESTDK1(tstKEY1)、並びに、第1～第3の開発用被暗号化鍵ESTDK1(EMK1(KEY1)), ESTDK1(tstMK1)およびESTKEY1(ESTDK1(tstMK1))をLSI20の開発者に提供する。

【0065】(第3の実施形態)図6は本発明の第3の実施形態に係る鍵実装システムの構成を示す図である。図6において、本実施形態に係る鍵実装システム3は、記憶部3aとLSI30とを備えている。記憶部3aは、最終鍵DK1を、内部鍵MK1を用いて暗号化して得た第1の被暗号化鍵EDK1(MK1)と、内部鍵MK1を、一方向関数による変換によって得た変換鍵CK1を用いて暗号化して得た第2の被暗号化鍵EMK1(CK1)とを、記憶している。

【0066】LSI30は、任意の定数Const1を記憶する定数記憶部31aを備えている。この定数記憶部31aによって種生成部31が構成されており、変換鍵CK1を生成するための元になる変換種として定数Const1は出力される。また、変換種となる定数Const1を、第1の入力IN1を用いて一方向関数によって変換し、変換鍵CK1を生成する一方向関数回路32と、第2の入力IN2を、一方向関数回路32の出力を鍵として用いて復号化する第1の復号回路33と、第1の入力IN1を、第1の復号回路33の出力を鍵として用いて復号化する第2の復号回路34とを備えている。

【0067】LSI30が鍵実装システム3に実装され

ると、記憶部3aに記憶された第1および第2の被暗号化鍵EDK1(MK1), EMK1(CK1)が、それぞれ、第1および第2の入力IN1, IN2としてLSI30に入力される。

【0068】このとき、LSI30は次のように動作する。すなわち、一方向関数回路32は、定数記憶部31aから出力された定数Const1を、第1の入力IN1すなわち第1の被暗号化鍵EDK1(MK1)を用いて、変換鍵CK1の生成に用いたものに相当する一方向関数によって変換する。これにより、一方向関数回路32から、変換鍵CK1が生成出力される。第1の復号回路33は、第2の入力IN2すなわち第2の被暗号化鍵EMK1(CK1)を、一方向関数回路32の出力すなわち変換鍵CK1を鍵として用いて復号化する。これにより、第1の復号回路33から、内部鍵MK1が生成出力される。第2の復号回路34は、第1の入力IN1すなわち第1の被暗号化鍵EDK1(MK1)を、第1の復号回路33の出力すなわち内部鍵MK1を鍵として用いて復号化する。これにより、第2の復号回路34から、最終鍵DK1が生成される。

【0069】ここで、例えば、内部鍵MK1をMK2に変更するものとする。この場合、記憶部3aには、まず、最終鍵DK1を新たな内部鍵MK2を用いて暗号化して得た第1の被暗号化鍵EDK1(MK2)を記憶させる。また、LSI30の定数記憶部31aに記憶された任意の定数Const1を、第1の被暗号化鍵EDK1(MK2)を鍵として用いて一方向関数によって変換し、新たな変換鍵CK2を生成する。そして、新たな内部鍵MK2を、新たな変換鍵CK2を用いて暗号化して得た第2の被暗号化鍵EMK2(CK2)を、記憶部3aに記憶させる。

【0070】このようにして記憶部3aに記憶させる第1および第2の被暗号化鍵を設定したとしても、上述したのと同様の動作によって、最終鍵DK1が正しく生成される。すなわち、LSI30に記憶された定数Const1を変更することなく、システム3内に記憶させる被暗号化鍵を、任意に設定することが可能になる。これにより、共通のLSIを用いて、システム毎に個別に、暗号化する鍵を設定することができ、このため、機密性をより高いものにすることができる。

【0071】図7は図6における各被暗号化鍵を生成する鍵生成の手順の一例を示す図である。図7に示すように、鍵管理者は、最終鍵DK1を、任意の内部鍵MK1を鍵として用いて暗号化し、第1の被暗号化鍵EDK1(MK1)を生成する(S31)。次に、定数Const1を、第1の被暗号化鍵EDK1(MK1)を鍵入力として用いて一方向関数による変換を行い、変換鍵CK1を生成する(S32)。その後、内部鍵MK1を、変換鍵CK1を鍵として用いて暗号化し、第2のEMK1(CK1)を生成する(S33)。そして、鍵管理者

は、第1および第2の被暗号化鍵EDK1(MK1), EMK1(CK1)を機器実装者すなわちシステム3の開発者に提供するとともに、定数Const1をLSI30の開発者に提供する。

【0072】システム3の製造時には、記憶部3aに、第1および第2の被暗号化鍵EDK1(MK1), EMK1(CK1)を記憶させるとともに、LSI30を実装する。

【0073】(第4の実施形態)図8は本発明の第4の実施形態に係る鍵実装システムの構成を示す図である。図8において、図6と共通の構成要素には、図6と同一の符号を付している。本実施形態に係る鍵実装システム4は、記憶部4aとLSI40とを備えている。記憶部4aは、第3の実施形態で説明した第1および第2の被暗号化鍵EDK1(MK1), EMK1(CK1)に加えて、第1の定数ID1をさらに記憶している。

【0074】一方、LSI40は、図6に示すLSI30における種生成部31に代えて、定数記憶部42と、第2の一方向関数回路43とからなる種生成部41を備えている。定数記憶部42は第2の定数Const2を記憶しており、第2の一方向関数回路43は第2の定数Const2を、第3の入力IN3を用いて一方向関数によって変換する。第2の一方向関数回路43の出力は、変換種として、一方向関数回路32に与えられる。

【0075】LSI40が鍵実装システム4に実装されると、記憶部4aに記憶された第1および第2の被暗号化鍵EDK1(MK1), EMK1(CK1)並びに第1の定数ID1が、それぞれ、第1～第3の入力IN1, IN2, IN3としてLSI40に入力される。

【0076】このとき、LSI40は次のように動作する。すなわち、種生成部41内の第2の一方向関数回路43は、定数記憶部31aから出力された定数Const2を、第3の入力IN3すなわち第1の定数ID1を用いて一方向関数によって変換する。これにより、種生成部41から、変換種Const1が生成出力される。一方、一方向関数回路32は、種生成部41から出力された変換種Const1を、第1の入力IN1すなわち第1の被暗号化鍵EDK1(MK1)を用いて、変換鍵CK1の生成に用いたものに相当する一方向関数によって変換する。これにより、一方向関数回路32から、変換鍵CK1が生成出力される。以降、第1および第2の復号回路33, 34の動作は、第3の実施形態と同様である。

【0077】図9は図8における各被暗号化鍵を生成する鍵生成の手順の一例を示す図である。図9に示すように、鍵管理者は、最終鍵DK1を、任意の内部鍵MK1を鍵として用いて暗号化し、第1の被暗号化鍵EDK1(MK1)を生成する(S41)。次に、第2の定数Const2を、第1の定数ID1を鍵として用いて一方向関数によって変換し(S42)、さらにその変換結果を、第1の被暗号化鍵EDK1(MK1)を鍵として用

いて一方向関数によって変換し、変換鍵CK1を生成する(S43)。その後、内部鍵MK1を変換鍵CK1を鍵として用いて暗号化し、第2の被暗号化鍵EMK1(CK1)を生成する(S44)。そして、鍵管理者は、第1の定数ID1と、第1および第2の被暗号化鍵EDK1(MK1), EMK1(CK1)を機器実装者すなわちシステム4の開発者に提供するとともに、第2の定数Const2をLSI40の開発者に提供する。

【0078】(第5の実施形態)図10は本発明の第5の実施形態に係る鍵実装システムの構成を示す図である。図10において、図6と共に構成要素には、図6と同一の符号を付している。本実施形態に係る鍵実装システム5は、記憶部5aとLSI50とを備えている。記憶部5aは、第3の実施形態で説明した第1および第2の被暗号化鍵EDK1(MK1), EMK1(CK1)に加えて、第1の定数ID1を、第1の被暗号化鍵EDK1(MK1)を用いて暗号化して得た第3の被暗号化鍵EDK1(MK1)をさらに記憶している。

【0079】一方、LSI50は、図6に示すLSI30における種生成部31に代えて、定数記憶部52と、第3および第4の復号回路53, 54とからなる種生成部51を備えている。第3の復号回路53は第3の入力IN3を、第1の入力IN1を鍵として用いて復号化する。定数記憶部52は、変換鍵CK1の生成元である変換種Const1を第1の定数ID1を用いて暗号化して得た第4の被暗号化鍵EConst1(ID1)を記憶する。第4の復号回路54は第4の被暗号化鍵EConst1(ID1)を、第3の復号回路53の出力を鍵として用いて復号化する。第4の復号回路54の出力は、変換種として、一方向関数回路32に与えられる。

【0080】LSI50が鍵実装システム5に実装されると、記憶部5aに記憶された第1～第3の被暗号化鍵EDK1(MK1), EMK1(CK1), EID1(EDK1(MK1))が、それぞれ、第1～第3の入力IN1, IN2, IN3としてLSI50に入力される。

【0081】このとき、LSI50は次のように動作する。すなわち、種生成部51内の第3の復号回路53は、第3の入力IN3すなわち第3の被暗号化鍵EID1(EDK1(MK1))を、第1の入力IN1すなわち第1の被暗号化鍵EDK1(MK1)を鍵として用いて復号化する。これにより、第3の復号回路53から、第1の定数ID1が出力される。種生成部51内の第4の復号回路54は、定数記憶部52に記憶された第4の被暗号化鍵EConst1(ID1)を、第3の復号回路53の出力すなわち第1の定数ID1を鍵として用いて復号化する。これにより、種生成部51から、変換種Const1が生成出力される。一方向関数回路32は、種生成部51から出力された変換種Const1を、第1の入力IN1すなわち第1の被暗号化鍵EDK1

1(MK1)を用いて、変換鍵CK1の生成に用いたものに相当する一方向関数によって変換する。これにより、一方向関数回路32から、変換鍵CK1が生成出力される。以降、第1および第2の復号回路33, 34の動作は、第3の実施形態と同様である。

【0082】図11は図10における各被暗号化鍵を生成する鍵生成の手順の一例を示す図である。図11に示すように、鍵管理者は、最終鍵DK1を、任意の内部鍵MK1を鍵として用いて暗号化し、第1の被暗号化鍵EDK1(MK1)を生成する(S51)。次に、変換種となる定数Const1を、第1の定数ID1を鍵として用いて暗号化し、第4の被暗号化鍵EConst1(ID1)を生成する(S52)。また、定数Const1を、第1の被暗号化鍵EDK1(MK1)を用いて一方向関数によって変換し、変換鍵CK1を生成する(S53)。その後、内部鍵MK1を最終鍵CK1を鍵として用いて暗号化し、第2の被暗号化鍵EMK1(CK1)を生成する(S54)。そして、鍵管理者は、第1～第3の被暗号化鍵EDK1(MK1), EMK1(CK1), EID1(EDK1(MK1))を機器実装者すなわちシステム5の開発者に提供するとともに、第4の被暗号化鍵EConst1(ID1)をLSI50の開発者に提供する。

【0083】(第6の実施形態)図12は本発明の第6の実施形態に係る鍵実装システムの構成を示す図である。図12において、図6と共に構成要素には、図6と同一の符号を付している。本実施形態に係る鍵実装システム6は、記憶部6aとLSI60とを備えている。記憶部6aは、第3の実施形態で説明した第1および第2の被暗号化鍵EDK1(MK1), EMK1(CK1)に加えて、内部鍵MK1を、テスト用変換鍵tstCK1を鍵として用いて暗号化して得た第3の被暗号化鍵EMK1(tstCK)を記憶している。テスト用変換鍵tstCK1は、変換鍵CK1の生成に用いられたものと同等の一方向関数によって変換されたものである。

【0084】一方、LSI60は、図6に示すLSI30といくつかの点で異なっている。

【0085】まず、第2および第3の入力IN2, IN3を入力とし、このいずれかを、テスト信号TESTに応じて選択出力する第1のセレクタ64を備えている。第1の復号回路33は、この第1のセレクタ64の出力を入力とする。

【0086】またLSI60は、図6における種生成部31に代えて、定数記憶部62と、第2のセレクタ63とからなる種生成部61を備えている。定数記憶部62は、変換鍵CK1の生成元である変換種IDfuse1と、テスト用変換鍵tstCK1の生成元であるテスト用変換種tstID1とを記憶している。定数記憶部62は、定数IDfuse1として、レーザトリミング等に

によるヒューズ切断により任意の値が実装可能に構成されている。第2のセレクタ63は、変換種IDfuse1およびテスト変換種tstID1のいずれかを、テスト信号TESTに応じて選択出力する。第2のセレクタ63の出力は、変換種として、一方向関数回路32に与えられる。

【0087】またLSI60には、第2のセレクタ63の出力を検証する検証回路65が設けられている。検証回路65は、定数IDfuse1に対する冗長演算の結果に相当する定数CRCfuse1がヒューズ実装された定数記憶部66と、第2のセレクタ63の出力に対して上述の冗長演算を行い、その結果と定数記憶部66に記憶された定数CRCfuse1とを比較する比較回路67とを備えている。

【0088】LSI60が鍵実装システム6に実装されると、記憶部6aに記憶された第1～第3の被暗号化鍵EDK1(MK1), EMK1(CK1), EMK1(tstCK1)が、それぞれ、第1～第3の入力IN1, IN2, IN3としてLSI60に入力される。

【0089】まず、LSI60の検査時における動作について説明する。この場合、テスト信号TESTは“1”に設定する。

【0090】このとき、第1のセレクタ64はテスト信号TESTとして“1”を受けて、入力IN3すなわち第3の被暗号化鍵EMK1(tstCK1)を選択出力する。また第2のセレクタ63は、テスト信号TESTとして“1”を受けて、定数記憶部62に記憶されたテスト用変換種tstID1を選択出力する。すなわち、種生成部61から、変換種としてテスト用変換種tstID1が出力される。

【0091】そして、一方向関数回路32は、種生成部61から出力されたテスト用変換種tstID1を、第1の入力IN1すなわち第1の被暗号化鍵EDK1(MK1)を用いて、変換鍵CK1およびテスト用変換鍵tstCK1の生成に用いたものに相当する一方向関数によって変換する。これにより、一方向関数回路32から、テスト用変換鍵tstCK1が生成出力される。

【0092】第1の復号回路33は、第1のセレクタ64の出力すなわち第3の被暗号化鍵EMK1(tstCK1)を、一方向関数回路32の出力すなわちテスト変換鍵tstCK1を鍵として用いて復号化する。これにより、第1の復号回路33から、内部鍵MK1が出力される。第2の復号回路34は、第1の入力IN1すなわち第1の被暗号化鍵EDK1(MK1)を、第1の復号回路33の出力すなわち内部鍵MK1を鍵として用いて復号化し、最終鍵DK1を生成する。

【0093】次に、LSI60の通常時における動作について説明する。この場合、テスト信号TESTは“0”に設定する。

【0094】このとき、第1のセレクタ64はテスト信

号TESTとして“0”を受けて、入力IN2すなわち第2の被暗号化鍵EMK1(CK1)を選択出力する。また第2のセレクタ63は、テスト信号TESTとして“0”を受けて、定数記憶部62に記憶された変換種IDfuse1を選択出力する。すなわち、種生成部61から、変換種IDfuse1が出力される。

【0095】そして、一方向関数回路32は、種生成部61から出力された変換種IDfuse1を、第1の被暗号化鍵EDK1(MK1)を用いて一方向関数によって変換する。これにより、一方向関数回路32から、変換鍵CK1が生成出力される。第1の復号回路33は、第1のセレクタ64の出力すなわち第2の被暗号化鍵EMK1(CK1)を、一方向関数回路32の出力すなわち変換鍵CK1を鍵として用いて復号化する。これにより、第1の復号回路33から内部鍵MK1が出力され、さらに検査時と同様に、第2の復号回路34から最終鍵DK1が生成される。

【0096】またこのとき、第2のセレクタ63の出力は、検証回路65内の比較回路67にも入力される。比較回路67によって、第2のセレクタ63の出力に対する冗長演算の結果と、定数記憶部66にヒューズ実装された定数CRCfuse1とが同一であるか否かがチェックされる。これにより、種生成部61に記憶された変換種IDfuse1の値の正当性も、併せて検証することができる。

【0097】図13は図12における各暗号化鍵を生成する鍵生成の手順の一例を示す図である。図13に示すように、鍵管理者は、最終鍵DK1を、任意の内部鍵MK1を鍵として用いて暗号化し、第1の被暗号化鍵EDK1(MK1)を生成する(S61)。次に、変換種となる定数IDfuse1を、第1の被暗号化鍵EDK1(MK1)を鍵として用いて一方向関数によって変換し、変換鍵CK1を生成する(S62)。また、定数IDfuse1を冗長演算(例えばCRC16)し、検証用の定数CRCfuse1を生成する(S63)。その後、内部鍵MK1を、変換鍵CK1を鍵として用いて暗号化し、第2の被暗号化鍵EMK1(CK1)を生成する(S64)。

【0098】同様に、テスト用変換種となる定数tstID1を、第1の被暗号化鍵EDK1(MK1)を鍵として用いて一方向関数によって変換し、テスト変換鍵tstCK1を生成する(S62)。その後、内部鍵MK1を、テスト変換鍵tstCK1を鍵として用いて暗号化し、第3の被暗号化鍵EMK1(tstCK1)を生成する(S64)。そして、鍵管理者は、第1～第3の被暗号化鍵EDK1(MK1), EMK1(CK1), EMK1(tstCK1)を機器実装者すなわちシステム6の開発者に提供するとともに、テスト用変換種tstID1, 変換種IDfuse1, 検証用定数CRCfuse1をLSI60の開発者に提供する。

【0099】(第7の実施形態)図14は本発明の第7の実施形態に係る鍵実装システムの構成を示す図である。図14において、図12と共に構成要素には、図12と同一の符号を付している。本実施形態に係る鍵実装システム7は、図12と共に構成からなる記憶部6aと、LSI70とを備えている。

【0100】LSI70には、図12における種生成部61に代えて、第1の定数記憶部72と、第2のセレクタ73と、第2の定数記憶部74と、第2の一方向関数回路75とを備えた種生成部71が設けられている。第1の定数記憶部72は、変換種IDfuse1の元になる第1の定数IDfuse2と、テスト用変換種tstID1の元になる第2の定数tstID2とを記憶している。第1の定数記憶部72は、第1の定数IDfusse2として、レーザトリミング等によるヒューズ切断により任意の値が実装可能に構成されている。第2のセレクタ73は、第1および第2の定数IDfuse2、tstID2のいずれかを、テスト信号TESTに応じて選択出力する。第2の定数記憶部74は、第3の定数Const3を記憶している。第2の一方向関数回路75は第3の定数Const3を、第2のセレクタ73の出力を用いて、一方向関数によって変換する。

【0101】また、検証回路65の定数記憶部66には、定数CRCfuse1の代わりに、第2の定数IDfuse2に対する冗長演算の結果に相当する定数CRCfuse2がヒューズ実装されている。

【0102】まず、LSI70の検査時における動作について説明する。この場合、テスト信号TESTは“1”に設定する。

【0103】このとき、第1のセレクタ64はテスト信号TESTとして“1”を受けて、入力IN3すなわち第3の被暗号化鍵EMK1(tstCK1)を選択出力する。また第2のセレクタ73は、テスト信号TESTとして“1”を受けて、第1の定数記憶部72に記憶された第2の定数tstID2を選択出力する。第2の一方向関数回路75は、第2の定数記憶部74に記憶された第3の定数Const3を、第2のセレクタ73の出力すなわち第2の定数tstID2を用いて一方向関数によって変換する。すなわち、種生成部71から、変換種としてテスト用変換種tstID1が出力される。

【0104】そして、一方向関数回路32は、種生成部71から出力されたテスト用変換種tstID1を、第1の入力IN1すなわち第1の被暗号化鍵EDK1(MK1)を用いて、一方向関数によって変換する。以降の動作は、上述の第6の実施形態と同様である。

【0105】次に、LSI70の通常時における動作について説明する。この場合、テスト信号TESTは“0”に設定する。

【0106】このとき、第1のセレクタ64はテスト信号TESTとして“0”を受けて、入力IN2すなわち

第2の被暗号化鍵EMK1(CK1)を選択出力する。また第2のセレクタ73は、テスト信号TESTとして“0”を受けて、第1の定数記憶部72に記憶された第1の定数IDfuse2を選択出力する。第2の一方向関数回路75は、第2の定数記憶部74に記憶された第1の定数Const3を、第2のセレクタ73の出力すなわち第1の定数IDfuse2を用いて一方向関数によって変換する。これにより、種生成部71から、変換種IDfuse1が出力される。

【0107】そして、一方向関数回路32は、種生成部71から出力された変換種IDfuse1を、第1の被暗号化鍵EDK1(MK1)を用いて一方向関数によって変換する。以降の動作は、上述の第6の実施形態と同様である。

【0108】またこのとき、第2のセレクタ73の出力は、検証回路65内の比較回路67にも入力される。比較回路67によって、第2のセレクタ73の出力に対する冗長演算の結果と、定数記憶部66にヒューズ実装されたCRCfuse2とが同一であるか否かがチェックされる。これにより、種生成部71に記憶された第2の定数IDfuse2の正当性も、併せて検証することができる。

【0109】図15は図14における被暗号化鍵を生成する手順を示す図である。図15に示すように、鍵管理者は、最終鍵DK1を、任意の内部鍵MK1を鍵として用いて暗号化し、第1の被暗号化鍵EDK1(MK1)を生成する(S71)。次に、第3の定数Const3を、第1の定数IDfuse2を鍵として用いて一方向関数によって変換し(S72)、さらにその変換結果を、第1の被暗号化鍵EDK1(MK1)を鍵として用いて一方向関数によって変換し、変換鍵CK1を生成する(S73)。その後、内部鍵MK1を変換鍵CK1を鍵として用いて暗号化し、第2の被暗号化鍵EMK1(CK1)を生成する(S74)。また、第1の定数IDfuse2に対して冗長演算(例えばCRC16)を行い、定数CRCfuse2を生成する(S75)。

【0110】同様に、第3の定数Const3を、第2の定数tstID2を鍵として用いて一方向関数によって変換し(S72)、さらにその変換結果を、第1の被暗号化鍵EDK1(MK1)を鍵として用いて一方向関数によって変換し、テスト用変換鍵tstCK1を生成する(S73)。その後、内部鍵MK1をテスト用変換鍵tstCK1を鍵として用いて暗号化し、第3の被暗号化鍵EMK1(tstCK1)を生成する。

【0111】そして、鍵管理者は、第1～第3の被暗号化鍵EDK1(MK1)、EMK1(CK1)、EMK1(tstCK1)をシステム7の開発者に提供するとともに、第1～第3の定数IDfuse2、tstID2、Const3と検証用定数CRCfuse2をLSI70の開発者に提供する。

【0112】(第8の実施形態) 図16は本発明の第8の実施形態に係る鍵実装システムの構成を示す図である。図16において、図12と共に構成要素には、図12と同一の符号を付している。本実施形態に係る鍵実装システム8は、図12と共に構成からなる記憶部6aと、LSI80とを備えている。

【0113】LSI80には、図12における種生成部61に代えて、第1の定数記憶部82と、第2のセレクタ83と、第3の復号回路84と、第2の定数記憶部85と、第2の一方向関数回路86とを備えた種生成部1が設けられている。第1の定数記憶部82は、第1の定数IDfuse2を、第1の被暗号化鍵EDK1(MK1)を用いて暗号化して得た第4の被暗号化鍵EIDfuse2(EDK1(MK1))と、第2の定数tstID2を、第1の被暗号化鍵EDK1(MK1)を用いて暗号化して得た第5の被暗号化鍵EtstID2(EDK1(MK1))とを記憶している。第2のセレクタ83は、第4および第5の被暗号化鍵EIDfuse2(EDK1(MK1)), EtstID2(EDK1(MK1))のいずれかを、テスト信号TESTに応じて選択出力する。第3の復号回路84は、第2のセレクタ83の出力を、第1の入力IN1すなわち第1の被暗号化鍵EDK1(MK1)を鍵として用いて復号化する。第2の定数記憶部85は第3の定数Const3を記憶している。第2の一方向関数回路86は第3の定数Const3を、第3の復号回路84の出力を用いて、一方向関数によって変換する。

【0114】また、検証回路の定数記憶部66には、定数CRCfuse1の代わりに、第4の被暗号化鍵EIDfuse2(EDK1(MK1))に対する冗長演算の結果に相当する定数CRCfuse3がヒューズ実装されている。

【0115】まず、LSI80の検査時における動作について説明する。この場合、テスト信号TESTは“1”に設定する。

【0116】このとき、第1のセレクタ64はテスト信号TESTとして“1”を受けて、入力IN3すなわち第3の被暗号化鍵EMK1(tstCK1)を選択出力する。また第2のセレクタ83は、テスト信号TESTとして“1”を受けて、第1の定数記憶部82に記憶された第5の被暗号化鍵EtstID2(EDK1(MK1))を選択出力する。第3の復号回路84は、第2のセレクタ83の出力をすなわち第5の被暗号化鍵EtstID2(EDK1(MK1))を、第1の入力すなわち第1の被暗号化鍵EDK1(MK1)によって復号化する。これにより、第3の復号回路84から、定数tstID2が输出される。第2の一方向関数回路86は、第2の定数記憶部85に記憶された第3の定数Const3を、第3の復号回路84の出力をすなわち定数tstID2を用いて一方向関数によって変換する。すなわち、

種生成部81から、変換種としてテスト用変換種tstID1が输出される。

【0117】そして、一方向関数回路32は種生成部81から出力されたテスト用変換種tstID1を、第1の入力IN1すなわち第1の被暗号化鍵EDK1(MK1)を用いて、一方向関数によって変換する。以降の動作は、上述の第6の実施形態と同様である。

【0118】次に、LSI80の通常時における動作について説明する。この場合、テスト信号TESTは“0”に設定する。

【0119】このとき、第1のセレクタ64はテスト信号TESTとして“0”を受けて、入力IN2すなわち第2の被暗号化鍵EMK1(CK1)を選択出力する。また第2のセレクタ83は、テスト信号TESTとして“0”を受けて、第1の定数記憶部82に記憶された第4の被暗号化鍵EIDfuse2(EDK1(MK1))を選択出力する。第3の復号回路84は、第2のセレクタ83の出力をすなわち第4の被暗号化鍵EIDfuse2(EDK1(MK1))を、第1の被暗号化鍵EDK1(MK1)を鍵として用いて復号化する。これにより、第3の復号回路84から、定数IDfuse2が输出される。第2の一方向関数回路86は、第3の定数Const3を、第3の復号回路84の出力をすなわち定数IDfuse2を用いて一方向関数によって変換する。これにより、種生成部81から、変換種IDfuse1が输出される。

【0120】そして、一方向関数回路32は、種生成部81から出力された変換種IDfuse1を、第1の被暗号化鍵EDK1(MK1)を用いて一方向関数によって変換する。以降の動作は、上述の第6の実施形態と同様である。

【0121】またこのとき、第2のセレクタ83の出力は、検証回路65内の比較回路67にも入力される。比較回路67によって、第2のセレクタ83の出力に対する冗長演算の結果と、定数記憶部66にヒューズ実装されたCRCfuse3とが同一であるか否かがチェックされる。これにより、種生成部81に記憶された第4の被暗号化鍵EIDfuse2(EDK1(MK1))の正当性も、併せて検証することができる。

【0122】図17は図16における被暗号化鍵を生成する手順を示す図である。図17に示すように、鍵管理者は、最終鍵DK1を、任意の内部鍵MK1を鍵として用いて暗号化し、第1の被暗号化鍵EDK1(MK1)を生成する(S81)。次に、第1および第2の定数IDfuse2, tstID2を、第1の被暗号化鍵EDK1(MK1)を鍵として用いて暗号化し、第4および第5の被暗号化鍵EIDfuse2(EDK1(MK1)), EtstID2(EDK1(MK1))を生成する(S82)。また、第3の定数Const3を、第1の定数IDfuse2を鍵として用いて一方向関数に

よって変換し(S83)、さらにその変換結果を、第1の被暗号化鍵EDK1(MK1)を鍵として用いて一方関数によって変換し、変換鍵CK1を生成する(S84)。その後、内部鍵MK1を、変換鍵CK1を鍵として用いて暗号化し、第2の被暗号化鍵EMK1(CK1)を生成する(S85)。また、第4の被暗号化鍵EIDfuse2(EDK1(MK1))を冗長演算(例えばCRC16)し、検証用の定数CRCfuse3を生成する(S86)。

【0123】同様に、第3の定数Const3を、第2の定数tstID2を鍵として用いて一方関数によって変換し(S83)、さらにその変換結果を、第1の被暗号化鍵EDK1(MK1)を鍵として用いて一方関数によって変換し、テスト用変換鍵tstCK1を生成する(S84)。その後、内部鍵MK1をテスト用変換鍵tstCK1を鍵として用いて暗号化し、第3の被暗号化鍵EMK1(tstCK1)を生成する。

【0124】そして、鍵管理者は、第1～第3の被暗号化鍵EDK1(MK1)、EMK1(CK1)、EMK1(tstCK1)をシステム8の開発者に提供するとともに、第3の定数Const3と、第4および第5の被暗号化鍵EtestID2(EDK1(MK1))、EIDfuse2(EDK1(MK1))と、検証用定数CRCfuse3とをLSI80の開発者に提供する。

【0125】(第9の実施形態)図18は本発明の第9の実施形態に係る鍵実装システムの構成を示す図である。図18において、図6と共に構成要素には、図6と同一の符号を付している。本実施形態に係る鍵実装システム3Aは、記憶部3bとLSI30Aとを備えている。記憶部3bは、図6の記憶部3aと同様に、最終鍵DK1を、内部鍵MK1を用いて暗号化して得た第1の被暗号化鍵EDK1(MK1)と、内部鍵MK1を、一方関数による変換によって得た変換鍵CK1を用いて暗号化して得た第2の被暗号化鍵EMK1(CK1)とを、記憶している。また、LSI30Aから入力される第3の被暗号化鍵を記憶するための空き領域38と、イネーブル状態とディセーブル状態とが切り替え可能に構成されたフラグflagとを備えている。

【0126】LSI30Aは、図6のLSI30の各要素に加えて、任意の定数IDfuseが実装可能なヒューズ回路35と、第2の復号回路34の出力を、ヒューズ回路35に実装された定数IDfuseを用いて暗号化する暗号回路36と、記憶部3bからの第3の入力IN3を、ヒューズ回路35に実装された定数IDfuseを用いて復号化する第3の復号回路37とを備えている。ヒューズ回路35はレーザトリミング等によるヒューズ切断によって、LSI30A毎に異なる定数が実装可能に構成されている。暗号回路36の出力は、第3の被暗号化鍵EDK1(IDfuse)として記憶部3bに送られる。

【0127】記憶部3bは、LSI30Aから第3の被暗号化鍵EDK1(IDfuse)を受けたとき、この第3の被暗号化鍵EDK1(IDfuse)を空き領域38に格納するとともに、第1および第2の被暗号化鍵EDK1(MK1)、EMK1(CK1)を消去する。そして、LSI30Aに対して第3の入力IN3として第3の被暗号化鍵EDK1(IDfuse)を出力する。また、フラグflagは、記憶部3bがシステム3Aに実装されたときはイネーブル状態であり、第1および第2の被暗号化鍵EDK1(MK1)、EMK1(CK1)が消去されると、ディセーブル状態になる。

【0128】LSI30Aがシステム3Aに実装されると、記憶部3bから、第1の被暗号化鍵EDK1(MK1)が第1の入力IN1としてLSI30Aに入力される。一方関数回路32は、種生成部31から出力された変換種Const1を、第1の入力IN1すなわち第1の被暗号化鍵EDK1(MK1)を用いて一方関数によって変換する。これにより、一方関数回路32から、変換鍵CK1が生成される。

【0129】第1の復号回路33は、第2の入力IN2すなわち第2の被暗号化鍵EMK1(CK1)を、一方関数回路32の出力すなわち変換鍵CK1を鍵として用いて復号化する。これにより、第1の復号回路33から、内部鍵MK1が生成される。第2の復号回路34は、第1の入力IN1すなわち第1の被暗号化鍵EDK1(MK1)を、第1の復号回路33の出力すなわち内部鍵MK1を鍵として用いて復号化する。これにより、第2の復号回路34から、最終鍵DK1が生成される。

【0130】この最終鍵DK1は、暗号回路36に与えられる。暗号回路36は、ヒューズ回路35に実装された任意の定数IDfuseを用いて最終鍵DK1を暗号化し、第3の被暗号化鍵EDK1(IDfuse)を生成する。生成された第3の被暗号化鍵EDK1(IDfuse)は、記憶部3bに書き込まれる。

【0131】このとき、第1および第2の被暗号化鍵EDK1(MK1)、EMK1(CK1)は記憶部3bから消去される。これとともに、フラグflagはディセーブル状態になる。

【0132】ここまで処理を製品出荷前に実行しておくと、記憶部3bには、LSI30A固有の定数IDfuseを用いて最終鍵DK1を暗号化して得た第3の被暗号化鍵EDK1(IDfuse)のみが記憶された状態で、出荷される。もちろん、製品出荷後に、電源を最初に立ち上げたときに、ここまで処理を実行するようにしてもらわないと。

【0133】そして、フラグflagがディセーブル状態のとき、記憶部3bからLSI30Aに第3の被暗号化鍵EDK1(IDfuse)が第3の入力IN3として出力される。すると、第3の復号回路37は、この第3の被暗号化鍵EDK1(IDfuse)を定数IDf

useを鍵として復号化して、最終鍵DK1を生成する。

【0134】このように本実施形態によると、暗号化に用いる定数がLSI毎に異なる場合であっても、最終鍵の暗号化を容易に実現することができ、機密性を向上させることができる。

【0135】なお、鍵生成の手順は、第3の実施形態と同様に、図7に示すように行えばよい。

【0136】(第10の実施形態)図19は本発明の第10の実施形態に係る鍵実装システムの構成を示す図である。図19において、図18と共通の構成要素には、図18と同一の符号が付してある。本実施形態に係る鍵実装システム3Bは、記憶部3bと、LSI30Bとを備えている。

【0137】LSI30Bは、図18のLSI30Aと比較すると、さらに、第2の一方向関数回路91およびセレクタ92を備えている。第2の一方向関数回路91はヒューズ回路35に実装された定数IDfuseを、種生成部31から出力された変換種Constを用いて一方向関数によって変換し、第2の変換種IDfuseCONを生成する。暗号回路36および第3の復号回路37は、定数IDfuseの代わりに、この第2の変換種IDfuseCONを鍵として用いて、暗号化および復号化を行う。またセレクタ92は、記憶部3bからの第3の入力IN3および暗号回路36の出力のうちのいずれか一方を、テスト信号TESTに応じて選択出力する。第3の復号回路37は、セレクタ92の出力を入力とする。

【0138】まず、実システム上における動作を説明する。実システム上では、テスト信号は“1”に設定する。

【0139】この場合、先の第9の実施形態と同様の動作によって、第2の復号回路34から、最終鍵DK1が出力される。暗号回路36は、第2の復号回路34の出力すなわち最終鍵DK1を、一方向関数回路91の出力すなわち第2の変換鍵IDfuseCONを鍵として用いて暗号化し、第3の被暗号化鍵EDK1(IDfuseCON)を生成する。

【0140】LSI30Bから出力された第3の被暗号化鍵EDK1(IDfuseCON)は、記憶部3bの空き領域38に格納され、さらに、第3の入力IN3として、LSI30Bに出力される。セレクタ92はテスト信号TESTとして“1”を受けて、第3の入力すなわち記憶部3bから出力された第3の被暗号化鍵EDK1(IDfuseCON)を選択出力する。第3の復号回路37は、セレクタ92の出力すなわち第3の被暗号化鍵EDK1(IDfuseCON)を、第2の変換鍵IDfuseCONを鍵として用いて復号化し、最終鍵DK1を生成する。

【0141】また、LSI30Bの検査時には、テスト

信号TESTは“0”に設定する。このとき、先の通常時と同様の動作によって、暗号回路36から、第3の被暗号化鍵EDK1(IDfuseCON)が生成される。セレクタ92はテスト信号TESTとして“0”を受けて、入力Bすなわち暗号回路36から出力された第3の被暗号化鍵EDK1(IDfuseCON)を出力する。第3の復号回路37は、第2の変換鍵IDfuseCONを鍵として用いてこの第3の被暗号化鍵EDK1(IDfuseCON)を復号化し、最終鍵DK1を生成する。

【0142】このように本実施形態によると、個別に異なる鍵が実装されたLSIを検査するときでも、検査パターンを変更することなく検査可能になる。

【0143】なお、鍵生成の手順は、第3の実施形態と同様に、図7に示すように行えばよい。

【0144】なお、本実施形態において、セレクタ92を省いてもかまわないし、第9の実施形態に係る図18の構成において、セレクタ92を設けてもかまわない。

【0145】また、第9および第10の実施形態において、種生成部は、他の構成、例えば図8、図10、図12、図14、図16に示すようなものであっても、かまわない。

【0146】

【発明の効果】以上のように本発明によると、LSI内の鍵とシステム上の鍵とを相互に暗号化することによって、鍵の相互関係と暗号方式の知識がないと解析が困難になるので、システム上において鍵の解析が困難になり、機密性および秘匿性が大幅に向上する。また、LSI開発者やシステム開発者は、被暗号化鍵のみを用いて開発することが可能となり、開発時における機密性を向上することができる。さらには、暗号化する鍵を容易に変更可能となり、システム個別に異なる鍵を与えることが容易になるので、機密性をさらに向上させることができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係る鍵実装システムの構成を示す図である。

【図2】図1のシステムで用いられる被暗号化鍵の生成手順の一例を示す図である。

【図3】本発明の第2の実施形態に係る鍵実装システムの構成を示す図である。

【図4】本発明の第2の実施形態に係るシステム開発時の機密鍵実装方法を示す図である。

【図5】図3および図4で用いられる被暗号化鍵の生成手順の一例を示す図である。

【図6】本発明の第3の実施形態に係る鍵実装システムの構成を示す図である。

【図7】図6のシステムで用いられる被暗号化鍵の生成手順の一例を示す図である。

【図8】本発明の第4の実施形態に係る鍵実装システム

の構成を示す図である。

【図9】図8のシステムで用いられる被暗号化鍵の生成手順の一例を示す図である。

【図10】本発明の第5の実施形態に係る鍵実装システムの構成を示す図である。

【図11】図10のシステムで用いられる被暗号化鍵の生成手順の一例を示す図である。

【図12】本発明の第6の実施形態に係る鍵実装システムの構成を示す図である。

【図13】図12のシステムで用いられる被暗号化鍵の生成手順の一例を示す図である。

【図14】本発明の第7の実施形態に係る鍵実装システムの構成を示す図である。

【図15】図14のシステムで用いられる被暗号化鍵の生成手順の一例を示す図である。

【図16】本発明の第8の実施形態に係る鍵実装システムの構成を示す図である。

【図17】図16のシステムで用いられる被暗号化鍵の生成手順の一例を示す図である。

【図18】本発明の第9の実施形態に係る鍵実装システムの構成を示す図である。

【図19】本発明の第10の実施形態に係る鍵実装システムの構成を示す図である。

【図20】対称暗号を説明するための図である。

【符号の説明】

1, 2, 3, 3A, 3B, 4, 5, 6, 7, 8 鍵実装システム

1a, 3a, 3b, 4a, 5a, 6a 記憶部
10, 20, 30, 30A, 30B, 40, 50, 60, 70, 80 LSI

11, 11A 鍵記憶部
12 第1の復号回路

13 第2の復号回路
14 第3の復号回路

15 第1のセレクタ
16 第2のセレクタ

31, 41, 51, 61, 71, 81 種生成部
31a 定数記憶部

32 一方向関数回路
33 第1の復号回路

34 第2の復号回路
35 ヒューズ回路

36 暗号回路
37 第3の復号回路

42 定数記憶部
43 第2の一方向関数回路

52 定数記憶部
53 第3の復号回路

54 第4の復号回路

62 定数記憶部

63 第2のセレクタ

64 第1のセレクタ

65 検証回路

72 第1の定数記憶部

73 第2のセレクタ

74 第2の定数記憶部

75 第2の一方向関数回路

82 第1の定数記憶部

83 第2のセレクタ

84 第3の復号回路

85 第2の定数記憶部

86 第2の一方向関数回路

91 第2の一方向関数回路

92 セレクタ

DK1 最終鍵

MK1 第1の内部鍵、内部鍵

KEY1 第2の内部鍵

EDK (MK1) 第1の被暗号化鍵

EKEY1 (EDK1 (MK1)) 第2の被暗号化鍵

EMK1 (KEY1) 第3の被暗号化鍵

EtstMK1 (tstKEY1) 第4の被暗号化鍵

EID1 (EDK1 (MK1)) 第3の被暗号化鍵

EConst1 (ID1) 第4の被暗号化鍵

EMK1 (tstCK1) 第3の被暗号化鍵

EIDfuse2 (EDK1 (MK1)) 第4の被暗号化鍵

EtstID2 (EDK1 (MK1)) 第5の被暗号化鍵

EDK1 (IDfuse) 第3の被暗号化鍵

EDK1 (IDfuseCON) 第3の被暗号化鍵I

Dfuse1 変換種

IN1 第1の入力

IN2 第2の入力

tstMK1 第1のテスト用内部鍵

tstKEY1 第2のテスト用内部鍵

tstCK1 テスト用交換鍵

tstID1 テスト用交換種

TA 第1のテスト信号

TB 第2のテスト信号

TEST テスト信号

CK1 変換鍵

Const1 定数(変換種)

ID1 第1の定数

Const2 第2の定数

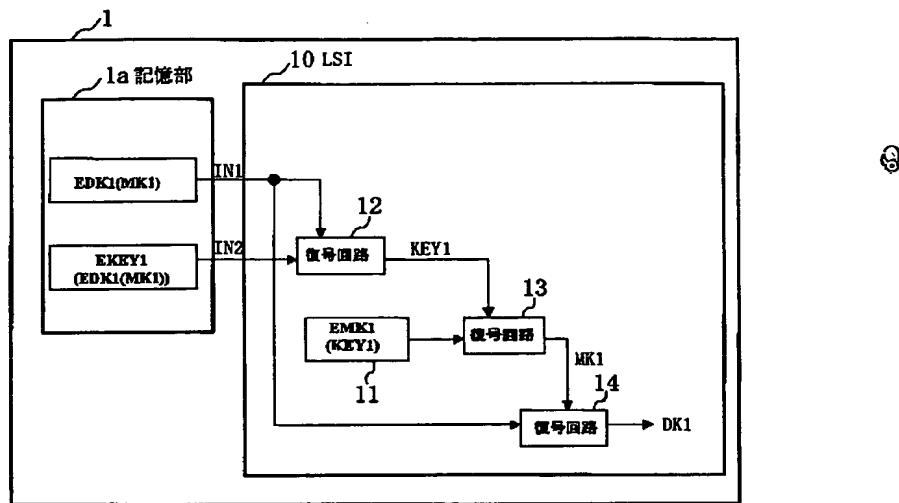
IDfuse2 第1の定数

tstID2 第2の定数

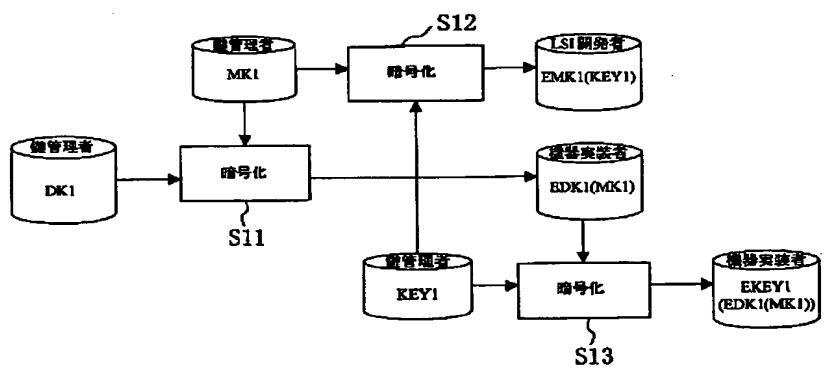
Const3 第3の定数

IDfuse 定数

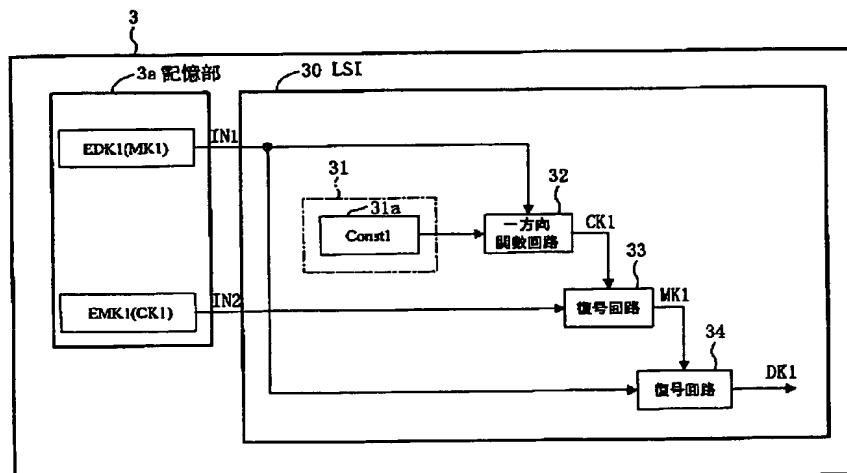
【図1】



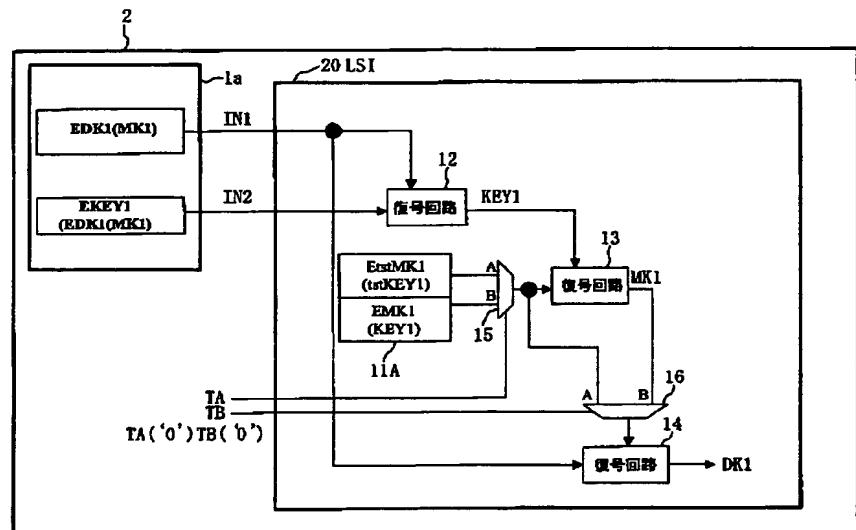
【図2】



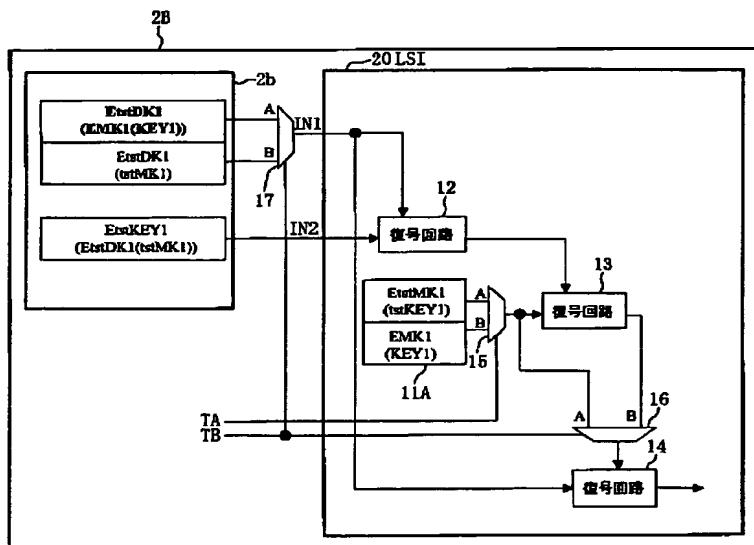
【図6】



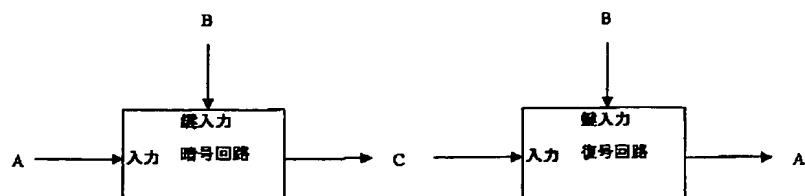
【図3】



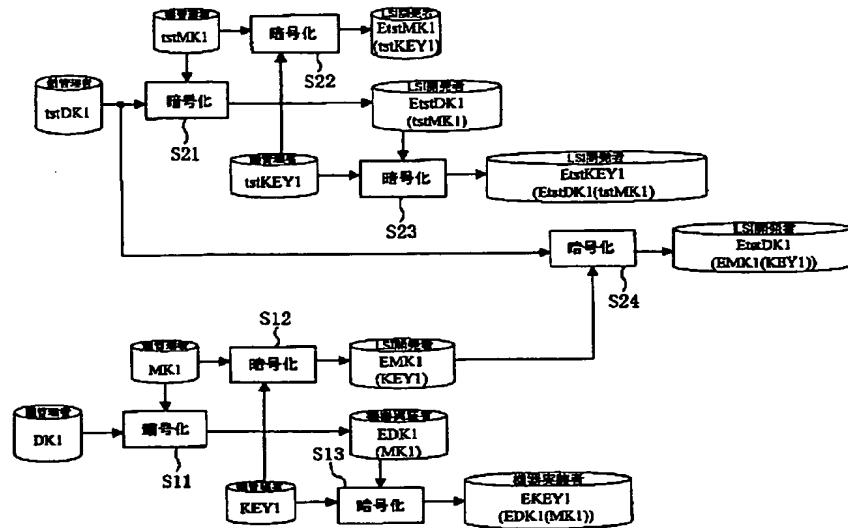
〔図4〕



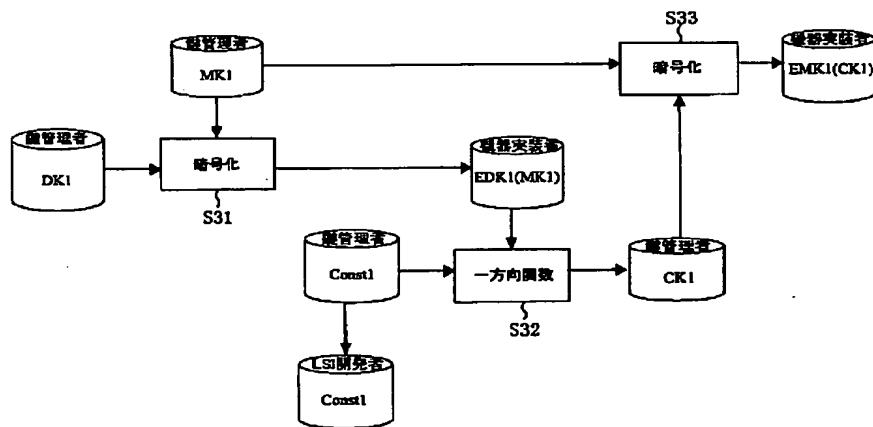
【图20】



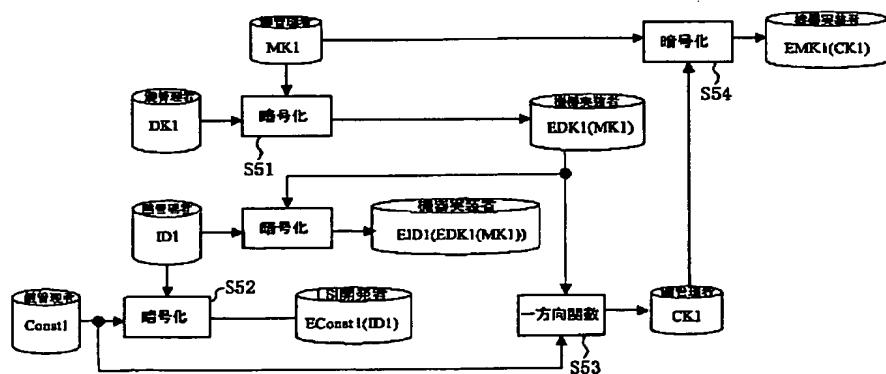
【図5】



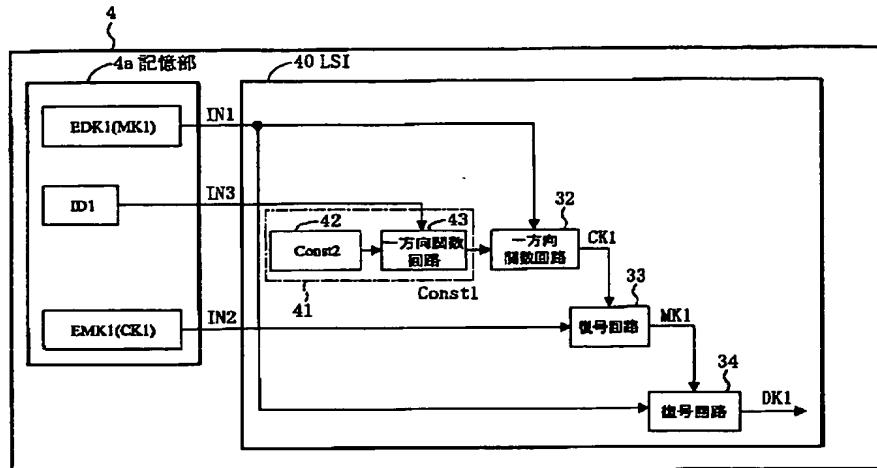
【図7】



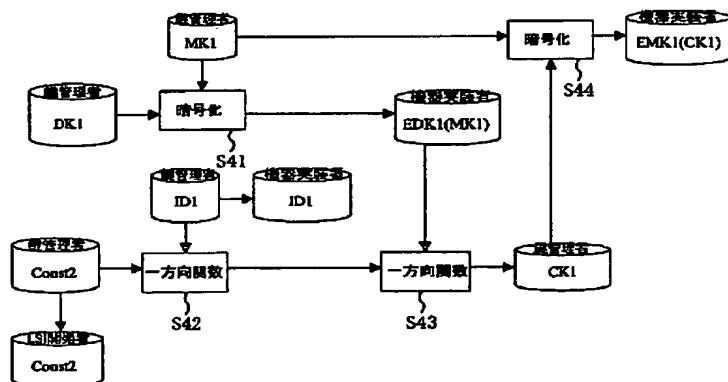
【図11】



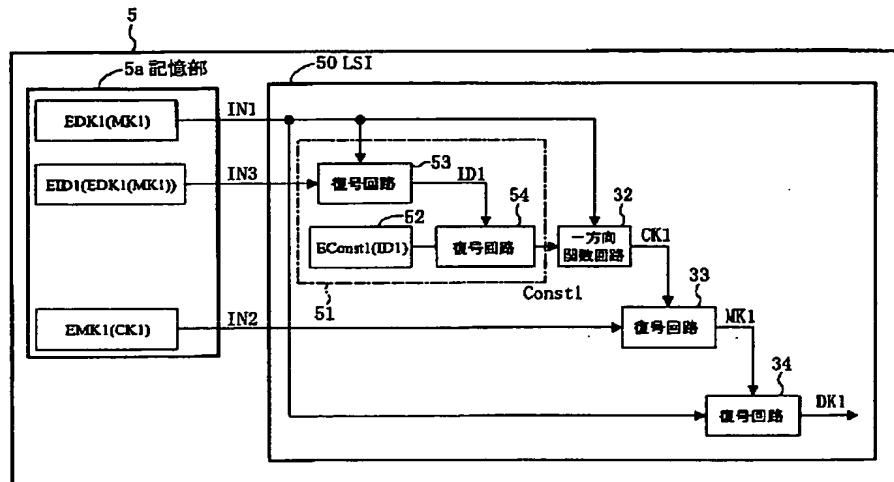
[図8]



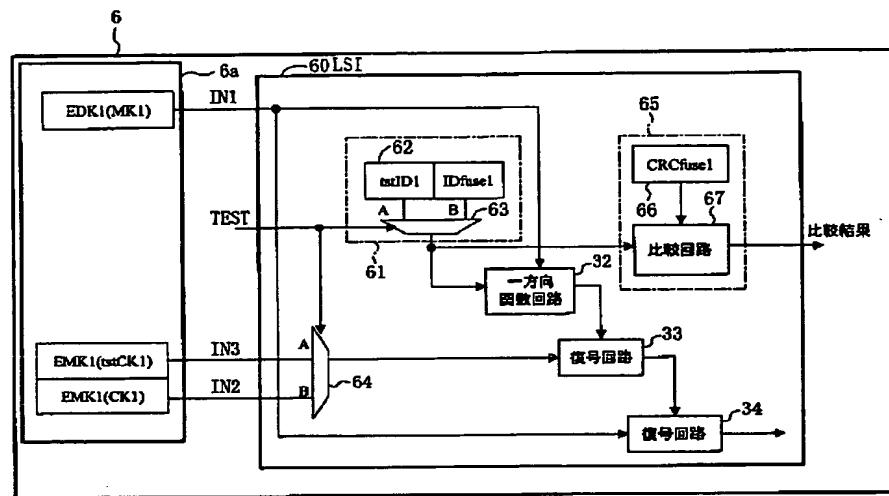
【图9】



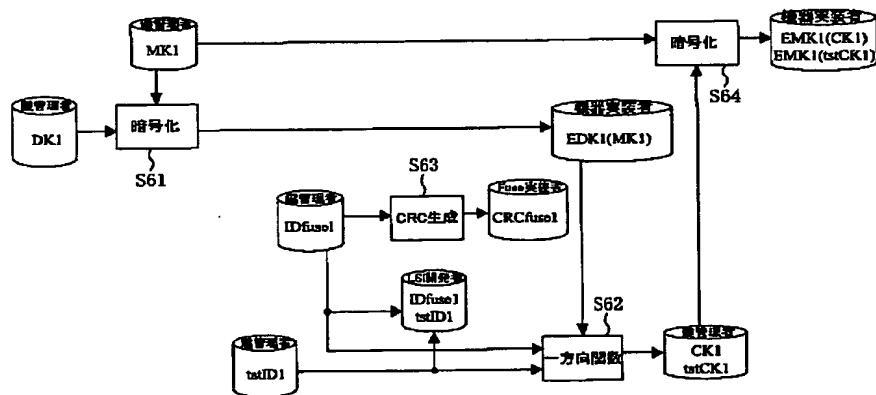
【図10】



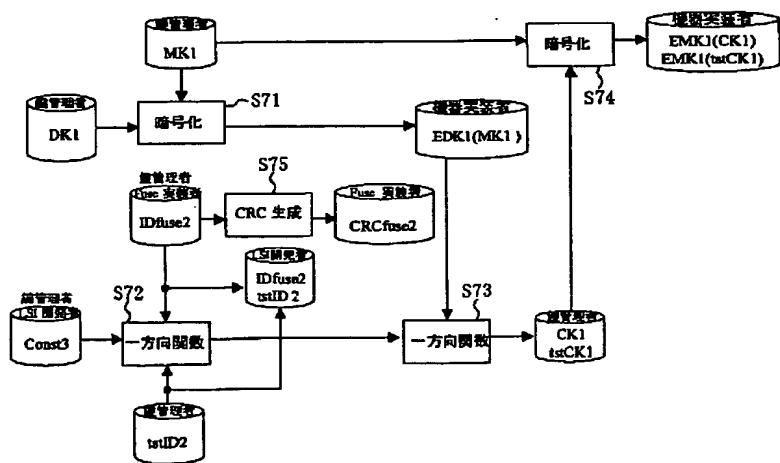
【図12】



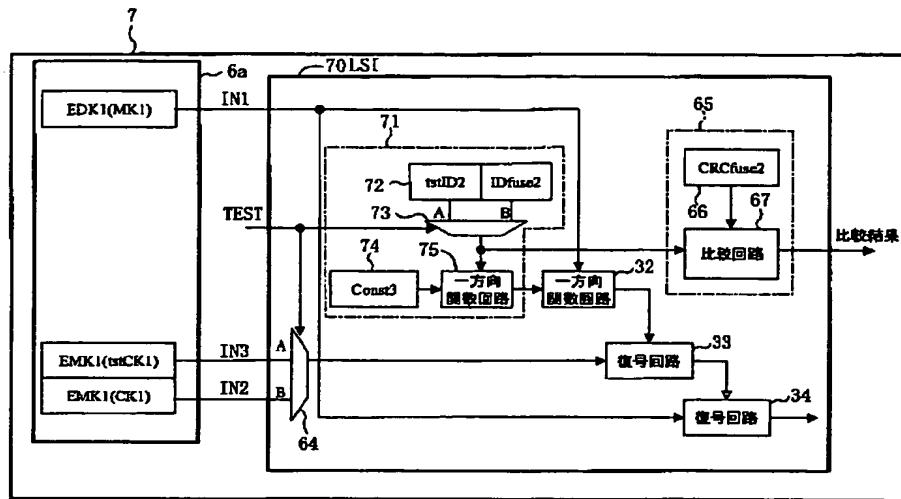
【図13】



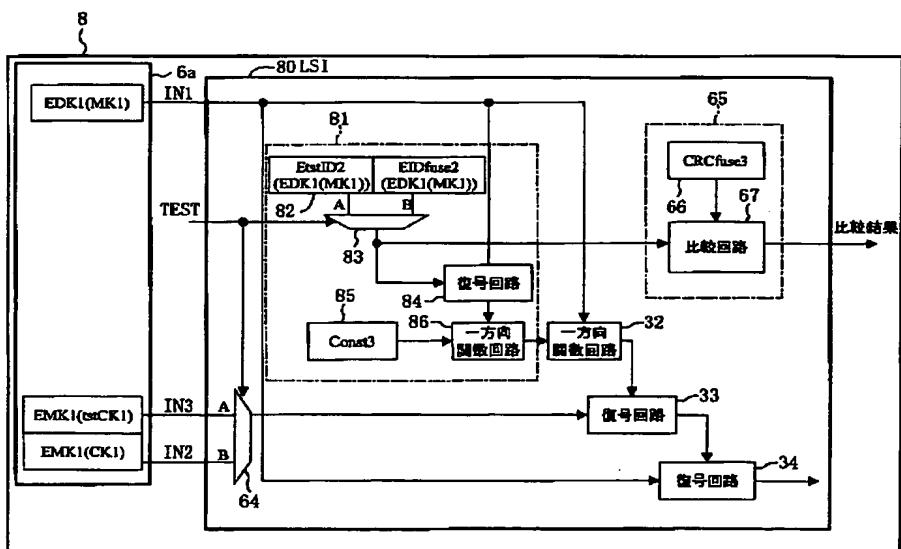
【図15】



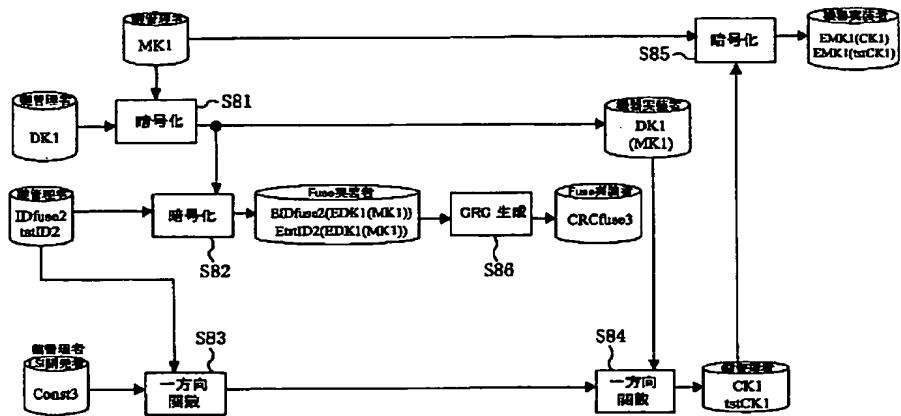
【図14】



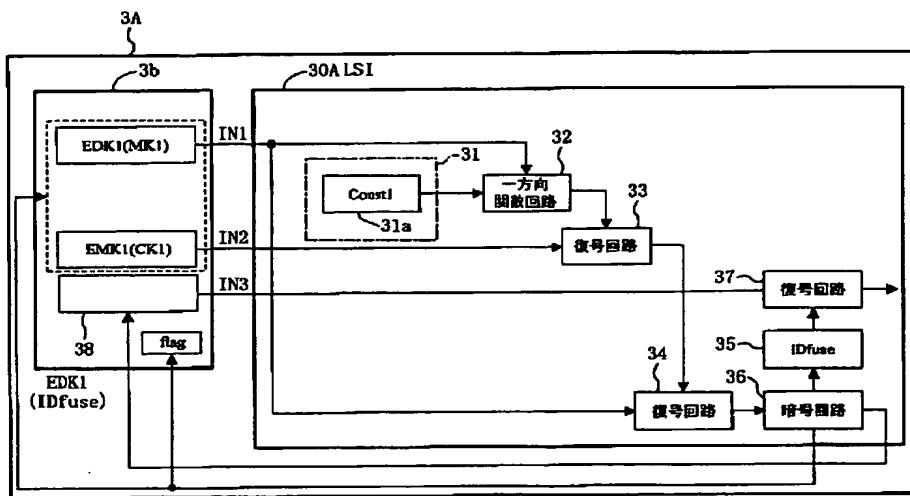
【図16】



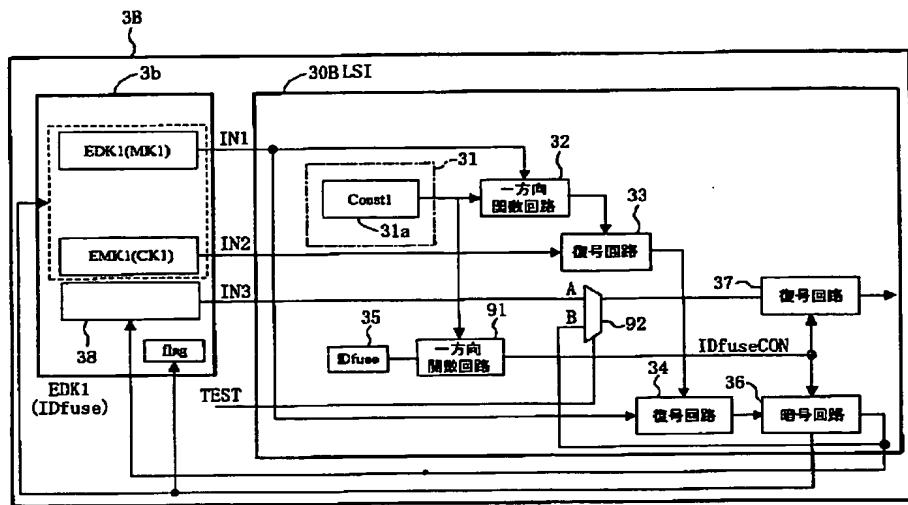
【図17】



【图18】



【図19】



フロントページの続き

Fターム(参考) 5B017 AA03 BA07 CA05
5J104 AA16 EA07 NA02 NA35 NA37
NA42